Brought to you by:

IBM

Secure Hybrid Cloud

for dummies®
A Wiley Brand

Fuel your transformation with hybrid cloud

Discover APIs to unleash core services

Optimize IBM Z® as a hybrid cloud platform

Judith Hurwitz

Daniel Kirsch

IBM Limited Edition

Secure Hybrid Cloud

IBM Limited Edition

by Judith Hurwitz and Daniel Kirsch

for dummies®
A Wiley Brand

Secure Hybrid Cloud For Dummies®, IBM Limited Edition

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

ISBN: 978-1-119-52795-4 (pbk); ISBN: 978-1-119-52798-5 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

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

Project Editor: Carrie A. Burchfield

Editorial Manager: Rev Mengle

Acquisitions Editor: Steve Hayes

Business Development Representative: Sue Blessing

IBM Contributors: Sherri Hanna, Mark Schultz, Rosalind Radcliffe, Kyle Charlet, Nathan Dotson, Diana Henderson, Dan Weigand

Production Editor: Magesh Elangovan

Table of Contents

INTRODUCTION 1
About This Book 1
Foolish Assumptions 1
Icons Used in This Book 2
Beyond the Book 2

CHAPTER 1: The Business Value of Hybrid Cloud 3
What Is Hybrid Cloud? 4
Hybrid Cloud as a Strategic Model 6
Understanding Why the Mainframe Is Essential to Hybrid Cloud Strategy 7

CHAPTER 2: IBM Z as a Secure Cloud Platform 9
Why You Need a Secure Cloud 9
The consequences of a data breach 10
The impact of reputational damage 10
Protecting Your Data 10
Accidental exposure 10
Insider attacks 11
Malicious third-party attacks 11
Regulations and compliance 11
What Does It Mean to Have a Secure Cloud? 12
IBM's Approach with Secure Cloud on IBM Z and LinuxONE 12
Pervasive encryption 13
Private cloud option 13
IBM Hyper Protect Services 14
The Importance of Ubiquitous Security Services 16

CHAPTER 3: Creating Agile Software on the Cloud through DevOps 17
Explaining the Value of Agile DevOps 17
Creating a Seamless DevOps Environment 18
DevOps in Practice 19
DevOps frameworks 21
DevOps and the cloud 22
DevOps in the World of Mainframes 23

CHAPTER 4: **Making Your Secure Cloud a Data and Application Hub** 27
Understanding the API Economy 28
The Value of the Mainframe as a Data and Applications Hub 29
The Mainframe as the Data and Application Hub 30
Data services 30
Application services 30
The Goal of the Mainframe Hub 31

CHAPTER 5: **Recognizing the Importance of Operational Insight** 33
The Importance of Cloud Predictability 33
Operational Intelligence in Action 34
Applying Machine Learning and Predictive Algorithms 35
Operational Intelligence on IBM Z 36

CHAPTER 6: **Getting Started with Your Enterprise Cloud Strategy** 37
A Cloud Strategy for the Enterprise 37
Planning Your Hybrid Cloud Strategy 38
Carefully assess requirements and limitations 38
Choose the right cloud deployment models 39
Determine the best workload and data localities 39
Understand and manage service levels, configurations, and licenses 40
Make governance a priority 40
Building the Z Cloud Foundation 41

Introduction

Welcome to *Secure Hybrid Cloud For Dummies*, 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 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, open APIs, and the inclusion of Kubernetes has made IBM Z a critical partner in the hybrid cloud world. Businesses can transform their IBM Z environments into a secure, private cloud. In addition, through IBM's public cloud, businesses may 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 important information throughout the book:


REMEMBER

This icon highlights important information that you should remember.


TIP

Tips help identify information that needs special attention.


WARNING

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

Beyond the Book

This short book can't offer every detail about a topic, so for more information outside the realm of this book, check out these topics:

- **Hybrid Cloud:** `http://ibm.biz/ZHybridCloud`
- **Data Security:** `http://ibm.biz/DataSecurity`
- **DevOps:** `http://ibm.biz/ZDevOps`
- **IT Operational Excellence:** `http://ibm.biz/ITOpExcel`
- **Z Case Studies:** `http://ibm.biz/ZCaseStudies`
- **The Connected Mainframe:** `http://ibm.biz/TheConnectedMainframe`

IN THIS CHAPTER

- Defining hybrid cloud
- Using hybrid cloud as a strategic model
- Powering your hybrid cloud strategy with the mainframe

Chapter 1
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 public or private cloud. Today, companies realize that continuous innovation requires supporting a variety of computing models.

Business disruption drives the need for hybrid cloud adoption. Across all industries, new competitors leverage technologies to move faster and with more agility than larger, well-established companies. These technologies benefit established organizations as well, by allowing them to build on their intellectual property, industry knowledge, and 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 traditional ways of delivering services. 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. A public cloud service can't always provide the necessary oversight to protect business integrity.

Hybrid cloud meets modern business demands with a distributed system that enables companies to select and leverage the right service for the task at hand. This environment is called the *hybrid cloud architecture* and is shown in Figure 1-1.

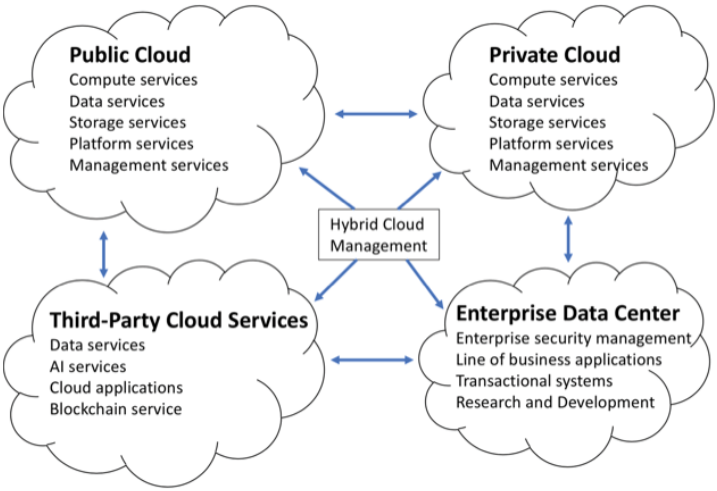


FIGURE 1-1: The hybrid cloud architecture.

REMEMBER

A hybrid cloud environment integrates traditional IT with a combination of public, private, or managed computing services to become a virtual computing environment. The goal of this environment is to balance service with flexibility to satisfy customer expectations. All services must be managed as if built to behave as a single unified environment.

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 the security of 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.

PUBLIC VERSUS PRIVATE CLOUD

All clouds aren't the same. Public cloud services are commercially available, and anyone can purchase a package of services on demand. Private cloud services live inside an enterprise data center, behind a firewall. Managed services can exist in either environment.

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.

The IBM Cloud Private (ICP) platform, for example, includes a unified installer to rapidly establish a Kubernetes-based cluster with master, worker, and proxy nodes. It is designed to manage and control applications that live within that environment.

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. The hybrid cloud approach allows each unit to select the appropriate cloud services for its needs. 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.

With the hybrid cloud, organizations can manage data, applications, business rules, and security services as a set of related capabilities and services. This approach enables a set of services to work together 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 multi-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

- Financial constraints and budgeting
- Security
- Scalability
- Operational management
- Integration with DevOps and DevSecOps environments
- Management of strategic 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 premise 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

The IBM Z mainframe is the key platform supporting hybrid cloud. It powers your hybrid cloud strategy by

- **Ensuring a consistent, stable environment:** With 99.999 percent 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.

IN THIS CHAPTER

- Seeing the rationale for the secure cloud
- Protecting your data
- Looking at the benefit of the secure cloud
- Leveraging IBM Z security services

Chapter 2
IBM Z as a Secure Cloud Platform

Managing data and intellectual property is imperative for businesses to survive and thrive. Therefore, security must be at the heart of any corporate strategy and plan. Customer and employee data must be protected both from a regulatory and a legal perspective. 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 is the top enterprise priority.

Why You Need a Secure 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 resides everywhere in your organization, including spreadsheets, documents, applications, and databases on premises and in the cloud. Therefore, security is no longer just the concern of the chief security officer. Security has become a major issue at the board level in all corporations. There are two key reasons for concern: the potential for data breaches and the resulting damage to the reputation of a company's brand.

The consequences of a data breach

A data breach can lead to catastrophic financial losses. 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 literally be ruined overnight if it fails to properly secure its intellectual property.

The impact of reputational damage

WARNING

Reputational damage can be almost as bad as direct financial and IP losses. Partners and customers are increasingly reevaluating the companies with which they choose to do business 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.

Take, for instance, a bank that's the victim of a highly complex and targeted cyberattack. Even if customers suffer no financial losses, they likely will reconsider banking with the company. If you have an account with the bank and are considering a home mortgage, would you really want to do business with the bank that was recently breached?

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 data. The majority of security 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 product of malicious actions. In fact, in many cases well-meaning employees or partners accidently expose data. In some instances, employees might use public cloud services that expose sensitive data to unauthorized users. For example, employees might 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 might be ideal for testing, they could expose private customer data.

Insider attacks

Although the vast majority of employees and contractors want to help the business, there may be bad actors that have malicious intentions. An employee may have recently been fired or overlooked for a raise or promotion. In some instances someone might 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. 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 might 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. In addition, nearly every business is rethinking its approach to security in light of the recent 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. For example, violating the PCI-DSS might mean that a retailer can no longer accept credit card payments.

What Does It Mean to Have a Secure Cloud?

There is 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.

TIP

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.
- Make sure that security is built into applications and data 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.
- Implement identity management into your hybrid cloud environment. In a complex multi-cloud environment, it is 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.

IBM's Approach with Secure Cloud on IBM Z and LinuxONE

One of the benefits of IBM Z is the significant level of security inherent in the platform. Often, businesses are concerned that putting their highly sensitive workloads in the cloud can put the company at risk. How do you balance the need for security with the flexibility of the cloud? We give you that information in this section.

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. In addition, the encryption doesn't require application changes.

You might 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 hardware to handle the encryption in an efficient and fast manner. The on-chip encryption processing can encrypt up to 13 gigabytes (GB) of data per second per chip.

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 later section "IBM Hyper Protect Services") or secure services in the IBM Cloud. In this next section we will discuss these options.

Private cloud option

IBM Z and LinuxONE servers can be configured to host the IBM Cloud Private software, a platform that integrates DevOps capabilities with cloud optimized software. IBM Cloud Private on Linux on IBM Z and LinuxONE allows teams to take advantage of the IBM portfolio of software via containers and microservices in a secure cloud environment. Deploying an IBM Cloud Private environment on a Linux on IBM Z or LinuxONE platform allows

customers to take advantage of mainframe's security services. For example, customers can automatically encrypt all their data, whether in flight or at rest, by using IBM Secure Service Container. This automatic encryption protects applications and data from attacks that attempt to gain access through privileged administrator credentials. Leveraging these security capabilities allows clients to securely build and host their own hybrid and private cloud deployments on premises.

IBM Hyper Protect Services

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, covered in the following sections, provides three services and intends to expand to include others that are crucial for providing protected cloud capabilities.

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 inputted data (the username, password, and so on) would be encrypted. However, there is a strong likelihood that the session is not 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, their system might provide a viable attack vector for criminals.

IBM Cloud Hyper Protect Crypto and Key Management

IBM Cloud Hyper Protect Crypto Services is a cryptography service designed to provide IBM-Z-based security capabilities to the cloud with a complete set of encryption and key management services with a dedicated namespace. IBM Hyper Protect Crypto Services helps to secure cloud native solutions for highly regulated industries through the highest level of security in a Hardware Security Module (HSM) ecosystem. The system provides high-density and unique transaction in-flight and at-rest protection accessible in the cloud on IBM Cloud Hyper Protect Crypto Services. This capability, typically used by banks and financial services companies, brings the security services of IBM Z to the IBM Cloud.

REMEMBER

IBM Cloud Hyper Protect Crypto Services integrates with multiple IBM Cloud data services such as IBM Key Protect, which is an IBM Cloud service that helps clients protect their keys on IBM Z. In addition, these services can be accessed with several popular programming languages including Java, JavaScript, and Swift.

IBM Cloud Hyper Protect Database Services (DBaaS)

IBM Cloud Hyper Protect DBaaS is a cloud service designed to provide databases on demand. One such database is MongoDB Enterprise Edition database clusters, which gives clients the ability to quickly provision, manage, and protect sensitive data workloads. The service leverages the LinuxONE pervasive encryption service, which helps retain clients' data in a fully encrypted database without needing specialized skills. In addition, it supports IBM Cloud Hyper Protect Containers (see the next section), enabling clients to deploy secure Kubernetes workloads. With IBM Cloud Hyper Protect DBaaS, clients can deploy database clusters in the IBM Cloud; manage database instances by using application programming interfaces (APIs), command line interfaces (CLIs), or user interfaces (UIs); administer database content; and monitor their database environments.

IBM Cloud Hyper Protect Container Services

IBM Cloud Hyper Protect Containers are deployed with a secure service container to provide Kubernetes clusters and a standardized way to package applications. This process enables portability and scalability in the IBM Cloud. The benefit of security at

the container level is increasingly important as this architecture becomes pervasive.

The Importance of Ubiquitous Security Services

As businesses move to cloud deployments at a rapid pace, they must provide security at all levels of the computing infrastructure. It simply isn't enough to assume that encrypting or security at a single layer will keep core assets safe. IBM Z security services provide a sophisticated source of protection — whether you leverage your own IBM Z private cloud platform or use the IBM Z cloud-based encryption and hyper protect services.

IN THIS CHAPTER

- Understanding the value of agile DevOps
- Creating a smooth DevOps process
- Looking at DevOps in practice
- Managing DevOps in a world of mainframes

Chapter 3
Creating Agile Software on the Cloud through DevOps

Cloud services have become a key foundation supporting businesses' ability to digitally transform quickly and efficiently. One of the benefits of both public and private clouds is the ability to provide 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.

In this chapter, we discuss how a multi-cloud environment has transformed DevOps so the organization can leverage the right platform based on security and data locality requirements.

Explaining the Value of Agile DevOps

The pace of business is constantly increasing, and businesses want ways to deliver value more quickly. For decades, IT departments have been searching for a predictable, secure, and flexible way to create, deploy, and manage applications. The growth of visual development methodologies, automated code generation,

and microservices based approaches are helping organizations. 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. Market dynamics and rapidly changing business demands are the ultimate drivers.

In the world of a highly distributed multi-cloud environment, DevOps has to produce software that's continually updated and managed. To be successful, application development needs 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 can no longer be created using a "siloed" development life cycle. Life cycle steps, including development, deployment, and test, can no longer be viewed as separate entities. Instead, they are integrated process steps with smooth transitions between them.

The desired outcomes of a DevOps practice are

- The acceleration of innovation, enabled through collaborative dedication to an integrated approach to the software development life cycle
- The CD of innovation via the automation of software delivery processes and greater development 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. The key is to leverage processes and techniques that support strong team collaboration and end-user involvement.

DevOps in 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.

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. The integrated DevOps cycle helps you bring people together with these practices rather than creating new silos. The parts of the cycle are as follows (as illustrated in Figure 3-1):

- **Continuous business planning:** Continual innovation requires an approach to business planning that is highly flexible to allow it to be responsive to customer feedback.

This step includes a perpetual way of grooming your backlog based on customer feedback, collaborative development, and continuous testing.

- **Collaborative development:** The obvious need for collaboration ensures that service requirements and service levels are met. Teams can build services and applications based on a microservices architecture. A focus on the customer experience at all stages of the life cycle keeps all stakeholders focused on a common goal.
- **Continuous testing:** 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.
- **Continuous release and deployment:** Keeping applications up to date is a necessary practice for businesses today and a key benefit of a DevOps approach. By continually releasing updates, teams can iteratively improve applications and respond to customer feedback.
- **Continuous monitoring:** By continually monitoring application performance throughout development, you can make sure they're ready for production deployment.
- **Continuous customer feedback:** With CD and the resulting fast pace of deployments, there's a critical need to receive and incorporate customer feedback. In addition, monitoring application performance in real time ensures that you meet customer expectations.

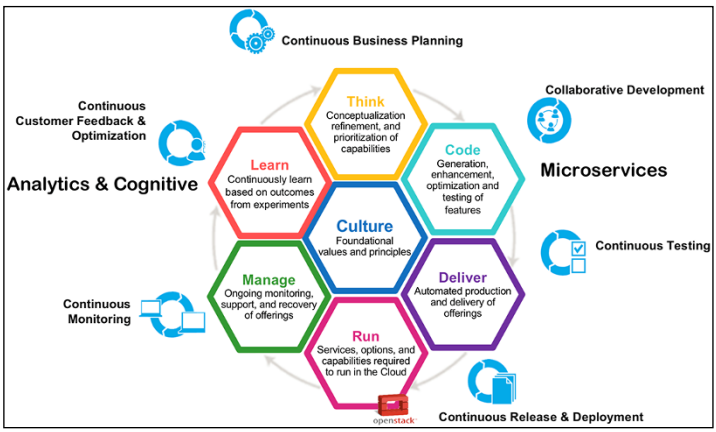


FIGURE 3-1: The DevOps cycle.

CONTINUOUS DELIVERY DOESN'T MEAN CHAOS

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 might be delivered to a staging environment before it is 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 mid-day, or you might impact the final calculations. In this staging scenario, you are 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 of 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 will be creating a culture of continual improvement no matter what platform you're working with. The same best practices will be effective across mobile apps, cloud services, and the mainframe. Therefore, you need to 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, it is effective for organizations to 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.

REMEMBER

While the Quality of Service (QoS) and capabilities of the platform you're deploying to can be different, the DevOps process can be the same. In fact, in many cases the DevOps tools and the pipeline will be the same no matter what platform you're using.

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.

DevOps in the World of Mainframes

We have seen that, as a business necessity, the new world of IT must be focused on continuous improvement and delivery (CI/CD) of applications. You may assume that mainframes do not 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 are a reliable option for hosting a variety of business applications. You can deploy a variety of applications on IBM Z. When you include Linux on IBM Z, you gain all 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 is not economically realistic (or necessary) from the perspective of cost and disruption to the business.


TIP

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.

- 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. Take the example of an existing banking system that has a full fraud detection system in IBM Z. The bank has built the fraud detection system and created custom rules to detect and stop potentially fraudulent activity. The system is fully optimized and performs at the speed and scale that's needed. All the bank's business knowledge is built into the system. This system is a huge competitive advantage over start-ups that must figure out how to create a fraud detection system from scratch.

New development processes, techniques, and tools exist that can assist in the modernization of mainframe applications. However, it is also important to recognize that the viability of the mainframe can mean that new applications can be developed for mainframes as well. Both new development and modernization of existing applications must take into account deployment to, or integration with, the cloud. Two types of applications are relevant here:

- **Cloud-native applications:** Also referred to as *cloud-first,* these applications are often built for mobile and web platforms, and therefore exhibit different dependencies that need to be considered in the development process versus more traditional applications. These applications tend to leverage web services and the microservices discussed here previously as a means of accelerating the development process. These applications will also need to be enabled with integration services focused on connecting mobile applications to backend services.
- **Cloud-enabled applications:** In this case, the traditional, mainframe-based applications were created to run within an organization's data center in order to support mission-critical business functions. Organizations have the ability to modernize the valuable assets within these applications though consistent APIs so they can work in concert with the new cloud-native applications built for systems of engagement with customers and other stakeholders. These applications are business critical and have many complex functions; therefore, they have more dependencies and require ongoing investment.

REMEMBER

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 — especially when these applications were written in COBOL. 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

  When you use the modern DevOps pipeline and tools for the mainframe that are used on other platforms, you are going to be able to achieve the speed and quality that the business needs. This approach enables businesses to support modern techniques, such as REST-based application programming interfaces (APIs).
- Building additional functions using Java and other modern languages, such as Swift 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
- Easing the migration from old compilers to new ones as seamlessly as possible

Additional requirements 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.

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, it is likely that operations staff will 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 is facilitated by a well-defined methodology.

IN THIS CHAPTER

- Cashing in on the API economy
- Seeing the value of the mainframe as a hub
- Understanding data and application services on the mainframe

Chapter 4
Making Your Secure Cloud a Data and Application Hub

The IBM Z platform is increasingly becoming core to the cloud strategy of many businesses that rely on the mainframe as the primary transactional engine for commerce with customers and partners. In addition, a large amount of complex business data resides on the mainframe. Some of this data is historic while other data sources are based on ongoing business transactions with customers. In addition, strategic mainframe-based applications are core to business operations. It is now possible to expose IBM Z services such as Information Management System (IMS) or Customer Information Control System (CICS) transactions so they can be consumed as cloud services. This new capability means that as we move into the world of hybrid computing, it's important that the mainframe be viewed as a strategic element of the overall cloud strategy.

In this chapter, you explore the approach needed to bring the mainframe forward as a hub for both data and applications. To be successful in this transition requires the use of application programming interfaces (APIs) and API management.

Understanding the API Economy

The API economy is transforming the way organizations can 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.

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 CICS, Db2, IMS data and applications, or Virtual Storage Access Method (VSAM) data as APIs with open standards and little Z subsystem knowledge.

IBM API Connect is an API management solution that 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 their application logic and their customer data.

At this point, you may be wondering how this approach to modern API management is different than Service Oriented Architectures (SOA). The emergence of SOA in the early 2000s was the beginning of a dramatic change in how enterprises began to build and consume services. However, in these early years, there were few standards and no management of the services or APIs. Without a well-planned management scheme, as the number of servers and

APIs grew, ensuring high quality and locating the correct services became challenging. The problem created by the lack of oversight and management of services and APIs has led to the creation of the API management platforms and the API economy.

The Value of the Mainframe as a Data and Applications Hub

Mainframe applications are the bedrock of many businesses. These applications often incorporate important business processes and rules that are fundamental to business operations. However, the code behind these applications is all written before modern coding standards and are therefore challenging to maintain or modernize. There is typically a lack of well-designed APIs that support integration with other services and other data sources. Likewise, mainframe data may be available in the data center but has not been put into a format that makes it easy for developers to access the data in a consistent manner. The mainframe architecture is purpose-built to be able to manage and execute on complex business processes at scale supporting a sophisticated level of security.

With modern tools, such as IBM's Application Discovery and Delivery Intelligence, that analyze code and discover dependencies, it is possible to refactor code so it can be modernized and evolve into a set of services that can become well-architected APIs. To be successful, businesses need to combine these rock-solid, secure systems of record with the flexible systems of engagement. Systems of engagement such as innovative services are applications that directly connect with customers to create a level of intimacy. For example, there may be travel services that help customers select hotels or other services through a mobile device. Likewise, financial services applications might engage with customers to provide data, such as account balances, in near real time.

By transforming mainframe applications through z/OS Connect Enterprise and IBM API Connect, the mainframe can expose APIs to connect with cloud-native applications that can consume these services, and mainframe applications with these exposed APIs can request and use cloud-native services as well.

The Mainframe as the Data and Application Hub

Connectivity between core systems of record, systems of engagement, and APIs is key to business success. The reality of business is that you need a combination of these systems of record that reside on the mainframe to interact with the systems of engagement that are typically cloud native.

TIP

To compete effectively in a changing business landscape, make sure that you have a hub to support the integration of data and application services. For many businesses, it's impractical to assume that you can move the massive amount of data and key application services from the mainframe to a cloud service. Using the mainframe platform as a hub for data and application services improves both security and performance of customer engagement.

Data services

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

Application services

Many mission-critical applications that reside on the mainframe have core rules and processes that are imperative to the consistent and predicable operations of the business. These application services can't easily be transferred to other applications and services without massive disruption. However, at times the applications need to be modernized. When these core applications are modernized, they can become the hub for business connectivity between systems of record and systems of engagement.

IBM provides an analytical platform to enable transformation of existing applications called Application Discovery and Delivery Intelligence (ADDI). The ADDI service is an analytical platform

intended to modernize applications. ADDI is designed to improve application services by helping you scan all your programs and the technology dependencies that surround the programs such as databases and third-party applications. 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.

After the analysis is complete, developers can more easily modernize existing code, transforming previously monolithic applications into services. At this point, RESTful APIs can be added so these services can be integrated and connected to cloud services to support business agility.

The Goal of the Mainframe Hub

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.

IN THIS CHAPTER

- Having cloud predictability
- Seeing operational intelligence in action
- Applying machine learning and predictive algorithms
- Gaining operational intelligence with IBM Z

Chapter 5
Recognizing the Importance of Operational Insight

Increasingly, Line of Business (LoB) leaders want to be able to control their interactions with customers and partners. But with this freedom comes responsibility. Those in charge are accountable for the Service Level Agreements (SLAs) that ensure operational integrity for the critical applications and infrastructure. Organizations must protect the performance and operations of the services across hybrid cloud platforms that are both predictable and manageable. Management must be able to understand and take quick actions based on the results of analytics in near real time in order to improve the customer experience.

In this chapter, we discuss how organizations can leverage operational and customer data for better insights into their hybrid cloud environments.

The Importance of Cloud Predictability

Increasingly, organizations are offering new services to manage customer interactions by opening the mainframe through new

cloud offerings. Managing this hybrid environment can't be done through manual processes. Simply too much complexity exists across too many platforms. The goal for the enterprise is to be able to provide the right services based on the service level and the security level to support corporate and government requirements. It is not enough to manage individual workloads; services need to be coordinated and managed.

When looking at managing cloud services, there are many options to consider when it comes to the performance of individual workloads. In a hybrid computing world, organizations often have to worry about a variety of platforms ranging from mainframes to departmental systems to public and private clouds. The challenge to offering business services to customers in a consistent and predictable manner is that those services often span silos in the IT organization.

One of the biggest issues for the IT organization is a lack of experienced specialists to support end-to-end visibility across all platforms. Each platform — whether it's a server, a mainframe, a cloud, or a network — has its own unique management services. To be successful, the operational team must demonstrate that they can increase user satisfaction and reduce costs while also maintaining operational integrity.

The objective of IT operational management is to ensure that all computing services behave in a predictable manner as though they were one unified computing environment. From an operations standpoint, the IT team must be able to support mission-critical transactional workloads that are growing at a rapid rate. These mainframe-based workloads must work seamlessly with a variety of hybrid cloud workloads.

Operational Intelligence in Action

Routine IT operational management issues can be handled through traditional automation techniques. Typically, conventional automation works well when you have a single, well-understood workload. However, when you begin managing multiple workloads across environments, make sure to provide an intelligent IT operations platform that enables management and control in a hybrid computing environment.

Today's IT operations leaders must manage not only the progressively complex physical environment but also increasingly large volumes of data — without a larger staff. It is not economically feasible to assume that your organization 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.

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. In addition, businesses are collecting more and more information about applications usage so they are in a better position to continually improve the user experience. To move to this predictive management environment requires that performance data be analyzed to understand the performance patterns.

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

In addition to the data generated about customers' experiences, each underlying system produces a massive amount of data about the health and operations of a software and hardware environment. However, this machine data is rarely used because there is simply too much information to easily gain actionable insights.

This data is generated by numerous systems spanning mainframes, virtual servers, cloud environments, storage devices, networking devices, and various sensors. Combining this data can provide context so that it can be used to take the best action to improve performance.

Therefore, the only way to effectively streamline management of IT operations is to apply machine learning and predictive algorithms. Through operational intelligence, the system is able to continuously monitor the behavior of the hybrid.

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 might 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 regarding 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

- **IBM Application Discovery and Delivery Intelligence (ADDI):** This service rapidly analyzes and visualizes the relationship between application components, data, and jobs in order to implement needed changes efficiently and safely. This service automates documentation. In addition, ADDI can identify and ensure the integrity of APIs.
- **IBM Common Data Provider for z Systems:** This solution provides access to the wide variety of IBM Z operational data by streaming it in near real time to multiple analytics platforms.
- **IBM Z Operations Analytics:** This solution provides insight into IBM Z operational data across multiple analytics platforms. It includes IBM zAware, which detects and diagnoses anomalies in IBM Z operational messages.
- **IBM Z APM Connect:** This solution provides visibility into transactions that span various IBM Z subsystems in multiple APM solutions.

Leveraging the IBM Z platform provides visibility, automation, and insights to manage multiple clouds when your hybrid environment includes the Z platform.

IN THIS CHAPTER

- Creating a cloud strategy
- Following the best practices for planning your hybrid cloud
- Building the Z Cloud foundation

Chapter 6
Getting Started with Your Enterprise Cloud Strategy

Most large enterprises rely on the mainframe as the center for high-volume and secure transactions. Because of the importance of mainframe applications and the stability, security, and performance of the platform, you need a robust hybrid cloud environment. The mainframe is transforming into a more flexible platform that supports the movement to enterprise security, containers, microservices, and the hybrid cloud. 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. Moving forward with this cloud strategy means addressing a variety of issues and demands.


TIP

Create a security fabric framework that works in the potentially more complex environment of the cloud. Mainframes provide 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

There are no shortcuts in planning for your secure 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 the five best practices in this section.

Carefully assess requirements and limitations

Businesses and IT must work closely together to determine what is actually needed from the cloud. 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? These and other questions need to be answered before a strategy and implementation plan for cloud can be created.

Choose the right cloud deployment models

The choice of deployment model is always an important consideration for organizations moving to the cloud. 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 and management 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 has never been more important. Now that there are so many options 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. It is often difficult to make the business case for architecting these applications. Furthermore, businesses are transforming their mainframes into hybrid cloud API hosts. What this means is that they're 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. One of the reasons why businesses are choosing to use IBM Z as an API host is that mainframe APIs will scale, will be highly available, and have the throughput necessary to meet end-user expectations.

While some applications might move to the cloud as part of a larger digital transformation effort, many new and existing mainframe applications will remain on IBM Z. Therefore, 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 are 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.

In a hybrid cloud situation, services may come from internal sources as well as one or more cloud providers. In order to manage these services effectively, configuration information must be gathered from all sources and reconciled and related to enable coherent and consistent service management. Varied information models for Configuration Management Databases (CMDBs), and the use of disparate tools to gather configuration details, make this management task challenging. Cross-platform tools, combined with configuration management policies that all providers must adhere to, can help here.

Finally, adding cloud can significantly increase licensing complexity due to the dynamic nature of the infrastructure and its "pay as you go" characteristics. Imagine a spike in demand that requires, say, a doubling of servers hosting a service. Predicting and licensing software in that situation is difficult, to say the least. There are a number of viable ways to manage licenses, including hosting applications, cloud-enabling current core systems, or leaving systems of record in place.

Make governance a priority

Organizations employing mainframes have governance procedures and policies on their mainframes designed to protect the integrity of their most critical data and applications. Trying to

replicate this well-planned 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, the organization's Line of Business (LoB) stakeholders, cloud providers, and even government entities. The result should be a governance framework that can ensure data and transaction integrity and protection.

Building the Z Cloud Foundation

Your Z cloud is not an isolated project to improve efficiency and increase flexibility. 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.

Cloud can be a major 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.

Notes

Notes

Accelerate digital transformation

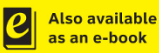
A secure hybrid cloud environment is critical for enterprises that need both on premises and public cloud services in order to meet the needs of their customers, partners, and suppliers. To thrive, businesses need to have a secure cloud across deployment models. The enterprise has a fiduciary responsibility to protect its intellectual property. 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
- Drive growth by leveraging the API economy
- 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 eight books, including Cognitive Computing and Big Data Analytics.
Daniel Kirsch, Principal Analyst, Hurwitz & Associates, is a researcher and consultant in cloud, machine learning, and security.

ISBN: 978-1-119-52795-4
Part #: 54017854USEN-00
Not For Resale



WILEY END USER LICENSE AGREEMENT

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