Compliments of IBM

IBM Limited Edition

Private Cloud

FOR DUMMIES®

Learn to:

- Make cloud computing an integral part of your business
- Perform in a smart and proactive manner
- Support collaboration between business and IT
- Leverage resources behind the corporate firewall

Judith Hurwitz
Marcia Kaufman

Private Cloud FOR DUMMIES®

IBM LIMITED EDITION

By Judith Hurwitz and Marcia Kaufman

John Wiley & Sons, Inc.

Private Cloud For Dummies®, IBM Limited Edition

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

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

ISBN: 978-1-118-15263-8

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction *1*

About This Book 1
Foolish Assumptions 2
How This Book Is Organized 3
Icons Used in This Book 3

Chapter 1: Building the Business Case for the Cloud . . . 5

Knowing What the Cloud Means to You 6
Helping the Business to Change through the Cloud 7
Journeying from Virtualization to the Private Cloud 7
How does virtualization add efficiency? 8
Starting with cloud computing through virtualization 9
Setting the Record Straight: What Is a Private Cloud? 9
Coming into the Picture: The Hybrid Cloud 11
Example 1: Commodity e-mail services 12
Example 2: Developing and testing a new application 12
Example 3: Using public cloud based sales automation with private clouds 13
Example 4: A public community cloud helps partnerships 13
Developing a Private Cloud Strategy 14

Chapter 2: Looking into the Foundations of Private and Hybrid Clouds 15

Getting Straight with Infrastructure as a Service 16
Looking into private IaaS 17
Dynamic provisioning, scheduling of resources 17
Dynamic provisioning and scheduling 18
Dynamic provisioning and scheduling in a private cloud 19
Self-service imperative: Business priorities and efficiency of the data center 20
Using IaaS in conjunction with the data center and other private cloud services 20

Expanding into Platform as a Service 21
Application development and execution services 22
Integrated lifecycle services 23
Workload management services 24
Data management services 25
Linking Business Services Together 26
Improving productivity 27
The Cloud as catalyst for business transformation 27

Chapter 3: Managing the Hybrid Cloud 29

Handling the Multi-Platform Environment 30
Common operational services 31
Federation of resources 32
Platform planning 32
The Service Level Imperative 33
Managing Workloads 34
The batch workload 35
The analytics workload 35
Transactional workloads 35
Putting Virtualization In Context 36
Managing Virtualization 36

Chapter 4: Locking Down Security and Governance 39

Understanding Security Risks 40
Alleviating the risks 40
Combining security requirements for private and public clouds 42
Assessing private cloud security requirements 42
Building a Secure Private Cloud 43
Ensuring data protection 43
Managing access and identity 44
Provisioning for secure environments 45
Controlling governance and audit 45
Dealing with intrusion 46
Looking into Best Practices for Securing the Hybrid environment 46
Evaluating the Risks and Creating a Cloud Security Strategy 48

Chapter 5: Integrating with and within Clouds 51

Understanding the Need for Cloud Integration 51
Looking at the Requirements for Cloud Integration 53
Connectivity 54
Transformation 55
Business logic 55
Management 56
Studying Cloud Integration Cases 57
Connectivity to clouds 57
Connectivity between clouds 58
Connectivity in clouds 58
Maintaining Governance and Security of Data 59
Securing access to data 59
Securing the connection 60

Chapter 6: Starting Your Cloud Journey 61

Looking into the Business Imperative for the Private Cloud 61
Defining the Role of IT 62
Considerations when Planning the Private Cloud 63
Business considerations 64
How is the business changing? 64
How does the company want to provide services in the future? 64
What are the financial constraints for the company? 64
Is the company too siloed for the strategy? 64
Is there an easy mechanism to encourage experimentation and innovation? 65
Implementation considerations 65
Evaluating reference architectures 65
Focusing on efficiency and flexibility 65
Planning for a fabric of services 65
Assuming that you'll plan for a lightweight approach 66
Monitoring and managing everything you do 66

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact `info@dummies.biz`. For details on licensing the *For Dummies* brand for products or services, contact `BrandedRights&Licenses@Wiley.com`.

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

Acquisitions, Editorial, and Media Development

Project Editor: Carrie A. Burchfield

Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Sr. Project Coordinator: Kristie Rees

Layout and Graphics: Melanee Habig, Christin Swinford

Proofreaders: Laura Albert, Jessica Kramer

Special Help: IBM Cloud Team

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Kathleen Nebenhaus, Vice President and Executive Publisher

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

About the Authors

Judith Hurwitz and **Marcia Kaufman** are cofounders of Hurwitz & Associates, a business technology consulting and research firm focused on cloud computing and the business value of technology investments. The team at Hurwitz & Associates have authored numerous *For Dummies* books.

Introduction

Welcome to *Private Cloud For Dummies,* IBM Limited Edition. Whether public, private, or hybrid, cloud computing is becoming an increasingly integral part of many companies' business and technology strategy. In an attempt to keep up with business innovation and change, companies are turning to flexible, elastic, and self-service computing resources that they can easily manage and scale in the cloud.

Cloud computing serves different needs for different constituents within your organization. For business leaders, cloud computing is a cost-effective way to leverage IT resources to prototype and implement strategic change. For your IT organization, the cloud is a platform that allows it to be significantly more proactive and responsive when it comes to supporting strategic business imperatives. While IT is leading the charge in focusing on best practices that support the balanced use of public, private, and data center resources — the emerging world of hybrid computing — don't lose sight of the fact that cloud is just as much about business model transformation as it is about technology transformation. In fact, many companies find that the cloud helps to support increased collaboration between business and IT leaders enabling them to more quickly adjust to changing market dynamics.

This book gives you some insights into what it means to create flexible pools of computing resources that break down silos in your company so you can perform in a smart and proactive manner.

About This Book

There has been a lot of confusion in the market about private and hybrid clouds — what they are and how they can be implemented to help the business get the benefits of the cloud while leveraging internal resources that are behind the corporate firewall. Many companies want to be able to have

pools of computing resources based on a self-service model where the company owns and operates those resources. With a private cloud model, these resources are standardized and automated. The reality is that most companies manage workloads across the data center, and public and private clouds — creating hybrid environments. This book helps put the private cloud model of computing into perspective for both business and technical leaders. In addition, the topics covered in this book are critical to the success of hybrid environments. If you like what you see in this book, you may like the full edition of *Private Clouds For Dummies* coming out in 2012.

Foolish Assumptions

This book is useful to many people, but we have to admit that we did pick a segment of the world to focus on for *Private Clouds For Dummies*. Here's who we think you are:

- You're already using various forms of cloud computing and are planning a long-term strategy. Perhaps we're preaching to the choir. You understand that the benefits of using all kinds of flexible cloud computing models represent sources of sustainable competitive advantage.
- You're a business leader who wants IT resources to be a utility that's optimized to leverage existing technology. You want IT to serve your business needs — you want to be able to execute your strategy on your timetable. You want IT to be your partner in innovating for the future.
- You're an IT leader who knows a lot about technology but aren't sure precisely how cloud computing — public, private, or a combination of the two as a hybrid model — works. You need to understand how cloud computing changes IT and what you need to do to support the business with cloud computing as an important enabler.

How This Book Is Organized

This book isn't intended to be an exhaustive technical manual on implementing and managing cloud computing. Rather, in this minibook, we give you a taste of the concepts and approaches you need to consider when embarking on your journey to the private cloud.

We've organized this book into six chapters:

- Chapter 1 gives you an overview of the business case for the private cloud — what it means to the business and exactly what a public, private, and hybrid cloud is.
- Chapter 2 provides you with an understanding of the technical foundation for private and hybrid clouds, including a discussion of Infrastructure as a Service, Platform as a Service, and Process as a Service.
- Chapter 3 delves into the issues of managing a hybrid environment and the workloads that need to be supported within that environment.
- Chapter 4 provides an overview of the security and governance issues you need to consider.
- Chapter 5 explains the approaches for integrating between and within cloud environments.
- Chapter 6 gives you a roadmap for planning your journey to the private cloud from a best practices perspective.

Icons Used in This Book

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

Tips help identify information that needs special attention.

Pay attention to these common pitfalls of managing your private cloud.

This icon highlights important information that you should remember.

This icon contains tidbits for the more technically inclined.

Chapter 1

Building the Business Case for the Cloud

In This Chapter

- Figuring out what the cloud means to you
- Changing business through the cloud
- Making the change from virtualization to the cloud
- Defining the private and hybrid clouds
- Coming up with a private cloud strategy

Cloud computing isn't just a group of computing resources sitting in a remote island. Rather the cloud is a computing model for enabling cost-effective business outcomes through the use of shared application and computing services. Increasingly, business leaders are using cloud computing to rapidly change business models and business processes. They are relying on cloud computing to experiment and impact revenue models. Cloud computing touches every aspect of the computing environment. It turns traditionally siloed computing assets into a shared pool of resources — so not only do you get to share servers, but you can also share networks, storage, applications, and services. And, when you share — everyone is a winner.

In this chapter, you discover the value of the private and hybrid cloud to your business. This chapter explains how cloud computing can help your business innovate without risking capital — thereby enabling you to experiment and pilot new business opportunities in a rapid fashion, identifying those ideas that work, but also crossing off the ideas that don't.

Knowing What the Cloud Means to You

Corporations are complicated — they're composed of a wide range of different people who have different responsibilities to make the business run like a charm. The value of the cloud is that it provides significant value no matter what your role in the business may be. So based on your responsibilities the cloud means different things. So who are you?

- If you're **a business user,** you'll want to have efficient access to IT resources when you need them without the red tape and delays.
- If you're **an application developer,** you want to have use of a platform that gives you development tools, middleware, and capacity so you have a well-tuned computing environment to help you focus on providing the best value for the business. You also want to put your skills to good use working on innovative projects instead of spending time configuring and reconfiguring complicated middleware.
- If you're **an IT operations manager,** you want to support an environment that can expand and contract based on business requirements. You want a safe and managed environment that has predictable workload management. And you want to keep business leaders happy.
- If you're **a business strategy planner,** you want to test out new business models without risk. You want a flexible environment that lets you try new business models without costly upfront investments.
- If you're **a member of the corporate management team,** you want to manage expenses and risks. You need to modulate your computing environment so you can maintain control over costs. You want your computing environment to be the nexus of your differentiation for supporting innovation to delight your best customers, suppliers, and partners.

Helping the Business to Change through the Cloud

Much confusion surrounds cloud computing and why it's becoming so important to business. The most obvious reason that businesses initially consider cloud computing is because business leaders want a more predictable and cost-effective way to acquire and manage computing resources. Business leaders want IT to be able to change their computing environments as quickly as their needs change.

For many organizations, public cloud services can fill a need for rapid access to affordable computing resources. Many businesses have begun to use Software as a Service (SaaS) offerings such as Customer Resource Management (CRM) to support their highly distributed sales teams. With these cloud-based applications, companies don't have to purchase their own hardware and supporting infrastructure. All the SaaS elements, including data, networking, storage, and management software, are operated by a third party. Likewise, this same company may find other SaaS applications that help with transaction management or data analytics. During peak periods, the company may use a cloud service to add more storage services for a short timeframe.

After business got a taste of the potential of cloud computing, business leadership began to understand that cloud computing could become a powerful engine of managing growth effectively. Therefore, business leaders are looking to transform their own data centers to support changing computing requirements. This boon has led to companies beginning to rethink the data center and the related services they need to have the flexibility and manageability the business and its constituents demand.

Journeying from Virtualization to the Private Cloud

Companies tend to incrementally move to the private cloud. Often this journey begins with virtualization. *Virtualization* is a technique for separating resources and services from the underlying physical delivery platform or environment. Why is it needed?

Most computer operating systems (including Linux and Windows) aren't designed to efficiently handle workloads. In fact, the typical server is terribly inefficient. In the old days, it didn't seem to matter very much. Server hardware was inexpensive, and if an application got bigger, the IT organization simply added more servers. But over time, all those servers made a mess of things. The servers took up a lot of floor space and used too much power. So companies discovered that with virtualization it was possible to abstract the hardware so it could be used more efficiently.

Therefore, virtualization is one of the most effective ways to reduce capital expenditures. Why is this true? Typically only less than 10 percent of an average server is used at any one time. Most of the time, these servers are sitting idle. After a company virtualizes its servers, utilization can be as high as 80 percent. So a lot of the compute resources that companies have invested in provide no benefit. Making matters worse, even those unused resources require a lot of manual management of the equipment.

How does virtualization add efficiency?

Virtualization has three technical capabilities that help with efficiency:

- It allows multiple operating systems and applications to be supported on a single physical system.
- It allows each of these virtual machines to be isolated from each other and from the physical hardware.
- It allows optimal utilization of the physical server resources.

With encapsulation, all the components needed to run an application can be put into a container so it runs without interference from other applications. With virtualization techniques, just about anything can be virtualized, including memory, networks, storage, hardware, operating systems, and applications. Virtualization platforms provide a set of resources and techniques for managing the efficient and secure operation of resources in an effective manner. This foundation enables greater utilization of the underlying hardware.

Starting with cloud computing through virtualization

Many IT organizations have had great success with virtualization. It has enabled them to get more efficient use of their resources and save money on hardware, floor space, and power. What's important about virtualization is that it helps companies take the first step toward a more efficient way to leverage their IT assets. Virtualization has enabled companies to decouple their assets from their physical platforms. It provides the right steps toward balancing workloads and moving those workloads to where they can be more efficiently used. But it doesn't go far enough. Cloud computing leverages the abstractions of hardware, software, applications, and storage and networks of the virtualization environment. In essence, virtualization now transforms physical silos into a pool of resources — one of the key principles of cloud computing. By beginning with virtualization, organizations focus on the management of resources. Without this focus on manageability, cloud computing is very difficult to implement.

Almost all vendors that sell public cloud services rely on virtualization as one of the techniques for optimizing their platform. Likewise, organizations implementing private clouds need virtualization to ensure that workloads are well balanced and well managed at the physical level. While virtualization itself is very valuable, it's only part of the solution. In fact, many companies assume that if they have implemented virtualization, they have a cloud. This isn't true. After virtualization has been implemented, you still need to standardize and automate how those virtualized workloads are managed. Combining virtualization with automating the delivery of those services creates a cloud platform.

Setting the Record Straight: What Is a Private Cloud?

In many situations a public cloud platform may not be the most appropriate environment for an organization. While companies like the freedom of the public cloud, they need more control, more security, and better flexibility. So companies typically adopt what's called a private cloud. What's a

private cloud? I'm glad you asked. A *private cloud* is a highly virtualized data center that sits behind a company's firewall. A private cloud is more cost effective for companies that already own a lot of computing resources. These same companies may have requirements for a higher level of security than can be guaranteed in a public cloud service.

What makes a private cloud different than a data center that includes some server virtualization? Check out these definitions:

- A private cloud includes automation of consistent processes and a self-service interface that allows internal developers to provision services on demand.
- A private cloud is highly automated in terms of how it manages pools of resources including everything from compute capability to storage, analytics, process management, and middleware.
- A private cloud offers a well-managed environment based on common services to improve the efficiency of the environment.
- A private cloud implements sophisticated security and governance capabilities specially designed for a company's requirements.
- A private cloud is owned and operated by a single company that controls the way services are expensed to various departments and partners.
- A private cloud controls the service level of the platform based on constituent needs and compliance requirements.

So what does this mean in the real world? Here is an example. A major retailer has managed its own traditional data center for the last 30 years. While in the beginning the environment was nice and neat, it has changed over the years. Originally, only a few computers existed and managing and self-containing them were relatively easy. However, that simple environment didn't last long. Over time, the company grew fast. It began purchasing new systems, new applications, new networking and the like. While there was a lot of scrutiny over which systems to buy, there was no way to control its growth. The requirement was simply to support the business needs for computing. Therefore, over the years the IT operation became increasingly complex and difficult to manage. When the business needed to change and provide new differentiated

services to its ecosystem of partners, it often took too long to execute. The pace of innovation slowed, and the company found that it was in danger of losing its competitive edge.

The CEO called a meeting of his executive team. It was time for a change. To make a very long, drawn out story short, the team decided that it would segregate its data center into two segments:

- One that included the many systems of record (accounting, specialized market software, and so on) that don't impact new business models. These systems all operate on a variety of hardware platforms, supporting many different types of middleware and operating systems.
- The other segment of the data center included analytics and application streaming workloads as well as the customer help desk. This segment was transformed into a private cloud. The company consolidated servers and implemented virtualization. It added a consistent operating system and middleware and development tools.

The entire environment was restructured so it could be optimized for performance. Self-service was added as the primary way that authorized users could access resources — based on authorization rules built into the private cloud. The IT organization decided to standardize on a set of development tools and platform, instituted as a standard for the software development organization. This eliminated the possibility of having too many different tools that made maintenance into a nightmare.

But the organization didn't stop there. They added business process management software so rules and processes that were required from a business model requirement could be implemented in software rather than on paper.

Coming into the Picture: The Hybrid Cloud

In reality, a private cloud doesn't exist in isolation from the rest of the data center and the public cloud. In fact, most organizations that adopt a cloud computing strategy discover that a hybrid approach fits well into their IT strategy. So what

does a Hybrid Cloud mean? A *hybrid cloud* is a combination of a private cloud foundation with strategic use of public cloud services. A hybrid cloud often leverages services that run within the data center as well. The best way to explain a hybrid cloud is to give you a couple of examples.

Example 1: Commodity e-mail services

A company may decide to use a public cloud service for a workload, such as electronic mail. Why is electronic mail such a good candidate for a public service? *Electronic mail* (e-mail) is a relatively simple application with a simple workload. Companies that specialize in public cloud e-mail services can optimize their hardware and software environment to support this type of workload. They can specialize in providing different levels of security — for a price. In reality, these companies can provide e-mail services for a fraction of the price that it costs to run and support an internal mail service. Even more important to many business executives is the fact that e-mail isn't a strategic service that adds value to the bottom line. As long as the e-mail vendor is trustworthy, companies are seeing the benefit of using this type of public cloud service. So a company with a private cloud often chooses a public e-mail service — thus the company's approach is a hybrid — combining some public services for capabilities that are commodity with private services based on the ability to deliver fast innovation to their ecosystem.

Example 2: Developing and testing a new application

Testing new applications can be a complicated task. To make sure that the application can work as advertised may require a lot of computing resources to simulate real world conditions. In the old days, companies used to acquire huge numbers of servers to conduct these tests, or they licensed software that simulated the usage of the application. With the advent of public cloud testing services, a company can leverage a testing-as-a-service environment on a one-time basis to make sure that the application performs as expected.

Likewise, a company may want to experiment with developing a new application. Instead of purchasing hardware, middleware, operating systems, and development tools, it may be more cost effective to develop that prototype application on a public cloud platform. If the prototype is successful and therefore strategic, the subsequent development could be moved to the private cloud.

Example 3: Using public cloud based sales automation with private clouds

There was a time when all sales automation software was implemented in the data center. With the advent of offerings, such as salesforce.com and SugarCRM, companies are increasingly discovering that it is practical to pay a per user per year price and leave the day-to-day management to a trusted vendor. But many companies also want to keep control over some of their most sensitive data. Therefore, they may choose to keep data about prospects on a public cloud. However, after those prospects become customers, they may now store that data in their private cloud. If a company is in a highly regulated market, such as financial services or healthcare, it may also want to keep that data on a private cloud.

Example 4: A public community cloud helps partnerships

At times, two or more companies partner on a strategic initiative. Instead of implementing a shared environment in one company's data center, companies increasingly rely on community cloud environments as a pragmatic meeting place. This community allows companies to move quickly to establish the components they need whether they are documents or statistics. After the collaboration is over, the companies no longer pay for the expanded resource.

Developing a Private Cloud Strategy

Before you begin your journey to the private cloud, you must establish a roadmap. If you don't know where you're going, you'll never get to your destination. Ask yourself the following questions:

- What do you want to do with your private cloud?
- Do you want to have a more flexible way to use your existing resources so that services can be provided with less overhead?
- Do you want to have a more proactive way to offer new innovative and revenue producing services to customers?
- What does your current environment look like?
- What are the characteristics of the workloads that you support?

After you understand your goals, you need to understand where you are today. Understanding your current environment helps you determine how to get started. For example:

- You may want to start with piloting a cloud service that demonstrates value quickly.
- You may want to start by virtualizing servers and adding automation to how those servers are managed.
- You may want to set up a self-service portal so developers can provision the required resources they need to start mission critical projects.

After you're able to prove business value, you can continue on your journey and truly impact the business.

Chapter 2

Looking into the Foundations of Private and Hybrid Clouds

In This Chapter

- Understanding infrastructure as a service
- Peering into platform as a service
- Managing business process as a service

The path to the private and hybrid models of computing require a well thought out and planned strategy. Many companies start their journey to the cloud by doing some server virtualization or selecting a few Software as a Service (SaaS) applications. While this approach can be pragmatic for getting some experience with cloud-based environments, it isn't sufficient in a competitive environment. To get true value from cloud computing requires a strategy for automating and standardizing a set of services around a collection of best practices that support a new level of innovation. By automating the routine functions, organizations can focus on new revenue opportunities.

In Chapter 1, we set the table for what a private cloud means for the business (go ahead and flip back there if need be). If you read that chapter, we hope that we've convinced you that there are some real benefits in leveraging this platform to transform your business by increasing the flexibility of computing. However, many different capabilities and services are required. In this chapter, we focus on the foundational technologies that should be part of your private and hybrid cloud strategy.

Getting Straight with Infrastructure as a Service

Infrastructure as a Service (IaaS) is one of the most straightforward cloud delivery models. IaaS is the delivery of computing services including hardware, networking, storage, and data center space based on a rental model. This means that the consumer of the service acquires a resource and is charged for that resource based on amount of resource used and the duration of that usage.

Many business units have discovered that they could easily bypass the IT department and use their corporate credit cards to provision IT services. For small temporary projects this can be a pragmatic and cost-effective solution. However, even at a few cents per CPU hour or Megabytes of storage, expenses can add up to significant cash. Those small amounts of money spread over dozens of departments add up to significant expenses. Even more complicated are issues related to the ability to track IT governance. If a business user creates important content through an IaaS service, there's no accountability. For example, almost no IaaS vendor will release usage logs to its customers. If a customer is storing data within a public IaaS platform, there's typically no way to determine where that data's being stored.

Life isn't black and white: there are always shades of gray. In many situations, a project isn't mission-critical or a company simply needs some extra resources for a project. For example, in a three-week period a development team may need extra storage, but purchasing physical storage systems for temporary needs makes no sense. Likewise, in some situations an online vendor may need extra computing and networking capabilities during the holiday rush. Purchasing extra system resources based on a short-term increase in demand for your products doesn't make economic sense, either.

Business users and IT developers are drawn to the ease of acquiring IaaS services. They simply go to a self-service interface and provide a credit card number, and an image of compute or storage services is provided almost instantly. The truth is that the traditional methods of acquiring computing resources simply haven't kept pace with business urgency.

But an alternative approach exists for companies who want to combine the flexibility of IaaS with the security, and resource management of a controlled IT environment are looking at private IaaS implementations. These private cloud implementations are often implemented in conjunction with public IaaS services in a hybrid manner.

Looking into private IaaS

Many companies are looking to implementing a private version of IaaS. In essence, a company creates a pool of resources that can be standardized and easily reused by the IT organization to complete projects. Why standardized? In an IaaS service, IT projects are created in predictable ways.

For example, a process may be designed to set up a test environment for code or provision storage to support an application. While certain nuances are different, 80 percent of the time the process within IaaS can be standardized. By standardizing these infrastructure services, the organization gains efficiencies, fewer inadvertent errors, and the ability to ensure consistency of managing the development lifecycle.

Another benefit of a private cloud service is overall manageability. One of the overarching benefits of IaaS is the ability to gain access to an image or copy of a set of resources that can be acquired via a self-service process.

While a public cloud vendor uses the self-service portal to ensure that the customer pays for the service, IaaS can be used differently in the private cloud. When a developer provisions a resource from a private cloud, IT management can make sure that when a project is completed, the resource (for example, compute resources or storage) is returned to the pool of resources. In this way, IT can better control what resources are available for projects and can control costs, utilization, and security.

Dynamic provisioning, scheduling of resources

Companies that operate IaaS for a living are much bigger than what you would see in the typical corporation. However, it is

quite reasonable that leveraging the right software in combination with your existing IT resources helps you create a version of your virtualized environment inside your own company.

What do you have to do? Well, before we tell you the secret, you have to understand the concepts behind dynamic provisioning and resource scheduling.

Dynamic provisioning and scheduling

Say that you're running an online retail site. You create a site that assumes you'll have about 100,000 visitors per day who browse and sometimes buy your wares. Your organization has many IT assets because its business value is directly related to its IT-based services. So the company created an internal self-service portal that allows developers to get the resources they need to keep the business running on the web. This internal service allows compute, storage, and networking resources to be dynamically allocated to the developer based on the project they're engaged in at the time. Those resources may be scheduled for use based on how critical that service is overall.

By enabling this rules-based, dynamic provisioning, the developers can more quickly manage their resources and acquire new ones at the right time without waiting. Because this dynamic provisioning is based on company policy based on the project, the developer is basically preapproved for use of the right resources. However, many companies design a workload management process that keeps priorities in check.

For example, if a critical application requires additional resources at the end of a fiscal quarter, the project being developed may have to be scheduled to leverage those resources at a different time or from a different pool of services.

Sometimes a need for services can't wait until those resources can be allocated. Spikes of demand for additional computing resources exist. For example, holidays, Christmas, or annual sales may cause your visitors spike to 300,000 in a single day. Rather than buy extra servers to accommodate peak loads, the company will rent some extra resources for the day or even a few hours — typically from a public cloud service.

This can happen because of software that automatically or dynamically allows those resources to be allocated.

In a public cloud IaaS, the customer visits a self-service portal and initiates a request for a certain amount of storage or CPU capacity. Once that user provides a valid credit card number, those resources are automatically allocated or provisioned to that user. When the user stops paying, those resources disappear.

Dynamic provisioning and scheduling in a private cloud

You want to be able to allow a developer to acquire more resources for a specific project without having to run out and buy more hardware. In essence, you create a pool of computing or storage resources that don't belong to one department or one application. You provide a self-service interface or portal for users. In addition, most organizations will add some rules that control what and how a developer can use these resources.

For example, a developer is working on a new project. He needs an extra terabyte of storage to get the project done. He goes to the self-service portal and requests a terabyte of storage. The system includes a rule that authorizes the programmer to get that storage. However, if he decides that it would be better to get two terabytes, the rules built into the system will reject that request. Even more important, after that project has ended, the system can be designed to release that terabyte of storage so it can be used for other purposes. In this way, a company can regulate how those resources and when resources are used.

Of course, this request could be done manually, but that isn't very practical or cost effective.

Establishing a dynamic provisioning model ensures that a company can codify rules and procedures. In addition, the scheduling capability makes sure that the pool of resources is managed in the most effective manner. Likewise, software within the computing environment manages the way all workloads are efficiently balanced. There will be times when one application must have priority for resources above another one. This type of resource scheduling is critical to the smooth operations of a dynamic computing environment.

Self-service imperative: Business priorities and efficiency of the data center

You can't have a discussion about the technical foundation of IaaS without understanding the imperative of self-service. The banking ATM service is a great example of the business value of self-service. Without the availability of the self-service ATM, banks would be required to use costly resources to manage activities of all their customers — even for the most repetitive tasks. With an ATM, repetitive tasks can be easily handled with a self-service interface. The customer makes a direct request to perform routine transactions that conform to predefined business rules.

For example, a customer must have an account to withdraw money. In addition, the customer can't take out more money than is in her account. There may be rules that dictate how much money an individual is allowed to withdraw from the ATM. This process is precisely how self-service works in the IaaS environment. In a private cloud environment, management can enable users to provision resources when they need them based on a set of predefined rules and business priorities. In this way, everyone is satisfied. The business also gets to control expenses and reduce capital expenditures. The business units have the freedom to avoid time consuming processes that slow down the ability to get the job done.

Many organizations that leverage IaaS opt for a hybrid approach — using both private services in combination with public IaaS services. Why is this approach attractive? A company can effectively leverage its own private cloud resources but use trusted public cloud services to manage peak loads. When organizations use this hybrid approach in a controlled way, it's effective. Control means that a company establishes rules for when and how business units can use an outside cloud service and therefore is better able to control costs. In addition, by implementing distinct usage rules, users can be prevented from storing sensitive data on a public cloud.

Using IaaS in conjunction with the data center and other private cloud services

Private clouds don't exist in isolation from the traditional data center and other cloud services operated by partners or

suppliers. In many situations, the private cloud services are used in conjunction with information that's managed within the data center.

For example, business units typically leverage the information from critical business applications, such as customer service applications, accounting systems, and product line systems. Companies often create a hybrid environment with their key trading partners based on a combination of data from the data center with a customized web-based system that may live in either a private or public cloud. Integration between clouds and data centers is a key component in success.

Expanding into Platform as a Service

In addition to leveraging compute, storage, network services in the form of IaaS, organizations expanding their use of cloud computing typically need a platform to create, deploy, and manage their cloud environment. This is true for companies building an application in the cloud that's deployed to a data center or for companies building a public or private cloud. An integrated environment that supports the development and management of cloud-based application is called Platform as a Service (PaaS).

What is PaaS? PaaS is an entire infrastructure packaged so it can be used to design, implement, and deploy applications and services in a public or private cloud environment. PaaS enables an organization to leverage key middleware services without having to deal with the complexities of managing individual hardware and software elements.

According to the National Institute of Standards and Technology (NIST), a U.S. federal government agency established to design technology standards, PaaS is the ability to provide a computing environment and the related development and deployment stack needed to deliver a solution to the consuming customer. This means that a computing environment PaaS requires a complete stack of development tools that are accessible via a web browser.

This abstracted (where the details of implementation are hidden from the user) stack is therefore designed to be cloud-based so the developer can use a self-service portal interface to create enterprise applications without having to acquire and deploy platform tools. In order to provide this level of abstraction, a number of components have to be included in a PaaS platform:

- Application development and execution services
- Integrated lifecycle services
- Workload management services
- Data management services

Application development and execution services

Application development and execution services are the heart of the PaaS environment. They're the anchor services that make the process of developing and executing applications in the cloud more streamlined. A PaaS platform provides the developer with a complete environment to design and develop applications. It includes the following services:

- Application design and development
- Application deployment
- Application Testing (such as load and performance testing)
- Middleware topology design and development
- Catalog of middleware components
- Application integration and connectivity
- Application and system health management (the integrity of the overall application)
- Runtime management to ensure execution of the application
- Application resources, including database and messaging
- Security and identity management
- Multi-tenancy so that each customer has a dedicated space isolated from other customer environments

These services make it possible for the developer to create applications without having to write to specific platform components (such as middleware and databases) because they're built into the platform. PaaS essentially enables the developer to build their applications, define their functional and non-functional requirements, and deploy their applications without having to deal with installing, configuring, or integrating middleware.

PaaS is built on virtualization that provides the ability to abstract the underlying services, such as middleware, operating systems, and hypervisors. Because of the virtualization of these services, each developer is provided with an image of the combined services. Therefore the developer doesn't have to deal directly with complex services and middleware — unless they want to be exposed to the details.

Developing in a PaaS environment is different than the way development organizations have designed software over the past few decades. In a traditional model, the development team may select a variety of different tools — operating systems, middleware, security products, and the like. If the team is very experienced this is a fine choice. Many organizations have been very effective with this approach. However, typically there are problems of managing complexity — especially in an era where more and more aspects of daily life are controlled by software. (Even the typical car has millions of lines of software.)

Integrated lifecycle services

While clearly developing applications and solutions for the cloud is different from building software intended for the data center, some commonalities exist. Like any good application development process, there needs to be a focus on managing the lifecycle. The integrated lifecycle services include

- Developer and tester collaboration services
- Application versioning
- Application configuration management

In PaaS environments, it's important to manage not only the development of an application but also the lifecycle of that application. While you can purchase an individual development

tool, the typical PaaS environment includes the software development tools, the testing environment, a workflow engine, configuration management, and applications management tools.

Because the PaaS lifecycle services are standardized, the development of consistent services is easier. For example, configuration management is built into the platform. Likewise, workflow regarding how the development lifecycle is intended to work is part of the environment. Developers have a self-service portal to provision additional services and to manage the development process across private and public clouds as well as within the data center. This can be accomplished through standardized templates (based on well-proven best practices) that predefine application services and how they relate to each other. These templates can be used to define who has access to which code based on roles and responsibilities. For example, middleware services provide a centralized way to control the deployment, management and monitoring of the development and deployment of applications.

Workload management services

One of the most important characteristics of building and deploying applications in the cloud is to be able to manage those workloads. A workload is an independent service or collection of code that can be executed. Two primary services for managing workloads exist in a PaaS environment:

- Dynamic workload management
- Fine grained Service Level Agreements (SLAs) to ensure that mission critical applications are given priority

In a well-designed PaaS environment, the critical elements need to be packaged so they can execute in the most efficient manner. But all workloads aren't the same. There are batch workloads (processing large amounts of data), real time workloads (real time data feed), and analytic workloads (analyzing complex customer information). For more information on workloads, check out Chapter 3.

In all types of cloud environments, it's typical that you'll have many workloads running in parallel. In the hybrid cloud, there

are complex integration and management issues. This is true because in a hybrid world there's the requirement to optimize cost and capacity requirements across different platforms — public, private, and data center. Therefore, it's important to make sure that these workloads are well balanced. There will be times, for example, where a specific application running in the cloud will need to be given more resources and priority over an occasionally used workload. This can be accomplished by tuning the hardware, operating system, middleware, development, and deployment environment as a unit. Tuning the environment can more effectively manage workloads. Therefore, this type of workload management has to be integrated into the PaaS environment. Without the ability to balance all types of workloads, the platform won't be practical in an enterprise environment.

Data management services

A typical cloud environment is tied not only to the data within a specific application but also in line of business applications running in the data center, e-commerce applications, and other customer facing environments. This data comes in all shapes and sizes. There may be transactional data, customer data, as well as various kinds of unstructured data based on everything from images to document content. Being able to manage the flow of this data is a critical issue in the PaaS environment. To accomplish this goal, the following services may be leveraged:

- Master data management (consistent definitions)
- Data integration and virtualization
- Data protection (ensuring security of the data)
- Data mobility (the ability to move data to where it's needed)
- Data quality

Some data may be stored in a SaaS application, such as a CRM application in a public cloud, while other data sources may be private and will be managed in the private cloud or within the data center. The PaaS environment provides data integration services that support integration between clouds, within the cloud, and between the cloud and on premises environments.

Linking Business Services Together

Each type of cloud contains a series of services that must be woven together to complete a business task. Whether you leverage a private cloud or a public cloud, or both, you need to have a way to intelligently manage the processes that make these environments a critical component in an evolving business strategy. What do we mean by this?

Business process thinking and awareness is fundamental to any type of cloud environment. It's important to understand the underlying processes that are an integral part of how your business is conducted. Some processes are so common that you may not even think of them as business process as a service. For example, many companies use an online service to handle payroll services. While there are elements of SaaS, the primary driving force behind this type of capability is process. Some employees are paid weekly or monthly. There's a process that's standardized based on a company's business rules. An employee's deductions based on taxes, social security, and his portion of benefits is automatically deducted from the amount the employee is paid. But other complexities are thrown in the mix.

In some situations, payment services must receive information from human resource systems that indicate changes in the employee's salary amount (deductions for a leave of absence, a commission payment, or a salary increase). In essence, the entire process of managing payments to employees becomes a set of business processes that are embedded into the hybrid computing environment. The accounting system that subtracts salaries from the cash on hand is managed in the traditional data center. The human resource system that keeps track of vacations, performance reviews, and other incentives are managed in a SaaS environment. The sales management system is yet another SaaS application that operates in the cloud.

The cloud has added a new layer of complexity to traditional business process management software (BPMS) because it's necessary to integrate many different applications and business services together to accomplish critical business tasks. These linkages typically need to be made across public

and private clouds and the data center. For more details on integration in the cloud, see Chapter 5.

The ability to manage business processes across clouds will continue to grow. Today we see common services, such as payment services, unified communications, collaboration services, and the like available within the cloud. Many organizations are increasingly leveraging these types of services not just for their internal needs but to create innovative business initiatives that involve partners, suppliers and customers.

Computing services are defined by the processes they support — whether they live in the data center, public or private clouds. None of these services live in isolation. They're becoming the tools to support new ways to roll out business innovation. In essence, with the movement to service orientation, companies are starting to think of their computing resources — no matter where they reside — as a set of assets that can be reshaped to create new business models.

Improving productivity

Companies are leveraging cloud computing to improve the productivity of their business process workflows. Many IT organizations are on a journey to streamline workloads by adding automation to traditionally stove-piped systems. In this scenario, IT takes on the role of abstracting the services that define the core of the business. This may involve creating business services that encapsulate processes used repeatedly throughout the business. IT may also take on the role of providing interfaces between systems of record with new services that may be cloud based. The net result is that both IT and business management can quickly and easily implement changes to vital business processes.

The Cloud as catalyst for business transformation

IT's new value-add consists of helping the business roll out new innovative processes that leverage the partner, supplier, and customer ecosystems in ways that improve the bottom line. To accomplish this objective requires that IT moves from

a focus on silos of systems to creating a set of services that can be linked together based on business process. In the new world, IT becomes a provider of abstractions and automation that enable the silos between systems to start breaking down.

What would this look like? Take an example of an insurance company that relies on partners — thousands of independent agents. Because the agents are independent, they're free to work with any company that offers them better ways to increase their revenue. The insurance company understands the challenge and knows that IT can be the secret to their success with agents. The insurance company created its own private cloud that was available only to its agents and their customers. The portal provides standard services such as billing, contracts, and other business processes that take time to create internally. However, this isn't unique. Many insurance companies offer these same back office functions to agents. To differentiate its services for agents, the insurance company provides the agent with a real time quoting and contract service. Because agents are able to provide a higher level of service than competitors, they remain loyal to the insurance company.

At the same time, this new approach gives the business the freedom and flexibility to experiment with new business models. For example, the insurance company built a new process that allowed partners to customize their own offerings. Without investing in any new hardware or software, the IT team created a new service and tested it with two partners. In the end, the service was too complicated and the experiment never became an offering. However, this experiment led to a completely different approach that became an important new revenue stream.

By creating business process oriented services that are cloud based, companies can implement revenue-producing offerings that become sources of sustainable competitive advantage for their partners.

Chapter 3

Managing the Hybrid Cloud

In This Chapter

- Managing multi-platforms
- Impacting business through the service level imperative
- Executing the right tasks: Managing workloads
- Dealing with virtualization at the hardware and application level

The idea of combining public and private clouds with data center capabilities into a hybrid computing environment is becoming the future. In the real world, not a single type of computing environment meets the needs of all users and all providers of services. Companies are becoming accustomed to the idea of using a Customer Relationship Management (CRM) system based on a Software as a Service (SaaS) model. The same companies have a private cloud for efficient software development and deployment of customer facing services. At the same time, the company uses public cloud services to handle workloads that require temporary resources.

Critical line of business applications and sensitive data remain in the traditional data center. While in isolation each of these services can be well managed. However, as the movement to this hybrid world becomes the norm, the ability to manage all of these services as a single unified computing environment will be mandatory. In this chapter, we provide insights into what it means to manage the workloads within a hybrid environment.

Handling the Multi-Platform Environment

Some people assume that cloud computing alleviates the necessity of worrying about hardware performance. Public cloud providers and outsourcing service providers handle this complexity behind the scenes. For these companies to be able to make money from cloud services, they must be able to optimize everything about their environments.

In fact, the most successful public cloud providers have spent a huge amount of effort to optimize their hardware platforms to efficiently support the types of workloads they support. So a public cloud e-mail provider views its servers combined with the operating system and middleware as a single unified platform that's optimized for e-mail workloads.

Another public cloud provider that offers an analytics service optimizes its overall systems environment so it's optimized for analytics, which is much more compute intensive when compared to e-mail.

The same requirements that make a commercial public cloud provider successful make a private cloud successful. In essence, implementing a private cloud must provide the business with the optimal environment that can support changing IT requirements. Because IT requirements are varied, one size doesn't fit all. An IT organization needs a variety of solutions — a hybrid of capabilities. Ironically while the hybrid model of computing solves many problems in terms of providing the most pragmatic approach to solve business problems, it adds to the complexity of management. Therefore, business and IT management need a well-architected strategy for supporting this level of flexibility. So what are the foundational issues that need to be addressed?

Three areas begin the journey:

- Common operational services across all platforms
- Federation of new resources into the system
- Planning to use the right platform for the right job

How the data center works

The typical data center includes many different hardware, software, operating systems, and applications. Unless your data center was built within the last few years based on a fully planned IT environment, most data centers have grown in an incremental fashion over many years. Each time a new application was needed to support the business a new set of servers would be purchased; each supporting its own set of services. Therefore, over many years the data center became a complicated and inefficient environment. While groups of servers and groups of applications are managed in silos, it does not provide end-to-end management. Server virtualization of the physical environment has helped to some degree but it doesn't go far enough. To gain efficiencies requires a degree of automation and consistency of services across the different supported platforms.

Common operational services

Several common operational services exist that are important to automate and standardize the virtualized environment. They include the following:

- Automated provisioning to automate the process of allocating resources to the right individuals at the right time in a well-managed way

  Automation helps by standardizing the rules for how and under what circumstances virtualized services can be used.

- Centralized cataloging of resources so that the user can easily find an application or a business service

  This catalog also includes information about the status of that service and how it can be used within the company.

When you begin to look at managing a hybrid environment, take a look at providing increasing levels of service automation management, such as automated provisioning of resources, simplified ways of accessing compute, storage, and network resources. You also need to be able to find and access the resources no matter where those services are located — you need some sort of service catalog that makes linking to the right resource at the right time much easier.

This catalog also provides the rules for usage and dependencies. By standardizing on this type of automation, managing these heterogeneous resources across workloads becomes easier for an organization.

Federation of resources

A hybrid environment calls for federating (linking distributed resources) computing resources so the right platform is used for the kind of workload being executed. In this way, when an application requires more compute cycles for a specific timeframe, those resources can be allocated from a public or private pool at runtime. Likewise, when a sales team uses a public CRM system, such as salesforce.com or SugarCRM, the team can select to move data about a new customer from the public site to a private database inside the data center. In some situations, the IT organization may use an external platform as a service to design a prototype of a new application to support a potential new line of business. If the partnership moves forward, that application will most likely move to a private cloud. Being able to support a federated environment provides flexibility to the business.

Platform planning

One of the benefits of establishing a hybrid model is the ability to use different technology approaches to match the workload to the right platform. For example, virtualization at the server, application, and image level can help streamline the use of resources. In this way, the IT organization doesn't have to anticipate precisely how the business may change over time. In essence, workloads can be targeted to run on the most appropriate platform. If the needs of that workload change, that workload can be moved to another platform that better supports the needs.

For example, an application has been designed to support a joint venture between three companies. Supporting the application requires a lot of compute and analytical resources. However, after a few years, the joint venture simply isn't as active and doesn't require the same platform support. Because the application was deployed via a hybrid environment, the workload can be redeployed to a different, less sophisticated platform.

The Service Level Imperative

How do you know what platform and what environment is right for your organization or your project? How do you know how fast or how powerful your IT services need to be? Service level decisions are always about tuning the environment to the business purpose. It's not sufficient to measure and monitor the performance of servers, networks, or virtualized images as individual components of your environment. You need to understand how they all work together to meet business objectives. In addition, you need to establish a process for monitoring and managing service levels that includes an awareness of the relative business priority of each of the business services supported by the environment.

With business services that may stretch across resources in the data center, and private and public cloud environments, performance monitoring requires a comprehensive view into all environments.

Establishing the right service levels for your business often requires negotiation based on business policies and economics. For example, sometimes the business may state that it wants the most power and the most reliability that money can buy. But, of course, no one has an unlimited budget. In fact, budgets for IT have never been tighter. So IT and the business may need to dig a little deeper into business requirements and expectations to determine how many resources to apply to a task. What does this mean? You need to calculate how the specific task or application impacts business results, and to do that, start with a few questions:

- How dependent is the business on the services? Is it an integral part of a commerce platform?
- How regularly is the service in use? Daily, every minute of the day? Or is the service used once a month or once a quarter?
- If the service performance degrades, will it impact revenue or customer satisfaction?
- How secure does the service need to be? Are there governance requirements that you're required to meet for your industry?

- Does the service create or use data that is subject to compliance requirements? What are your processes for monitoring and tracking the movement of these data?
- Does the service have to be available at all times?
- What's the impact of performance on customer satisfaction?
- What's the impact of performance on business goals and objectives?

The answers to these questions can change over time because business tends to be dynamic. Creating a hybrid environment consisting of public, private, and data center resources gives you a lot of options to help meet changing business needs. If you establish the right service management plan, you can manage the workloads based on the importance of those workloads to the business.

How will you know whether you have tuned your environment to support the desired service level? In order to know, do you need to monitor and measure the performance of the services within your hybrid environment? This process is easier for services that you control within the private cloud or the data center itself. Managing an environment is more difficult when you include public cloud services, such as SaaS applications within your hybrid environment.

Most third party service providers allow you to gain visibility into performance statistics. However, they rarely allow you to have granular access to the performance of these applications. Sometimes the SaaS vendor's ecosystem includes third party monitoring and management products that allow you a better ability to monitor the overall service level of your hybrid environment.

Managing Workloads

In a hybrid environment, many different workloads serve the needs of different business requirements. So what's a workload? A *workload* is an independent service or collection of code that can be executed. In essence, the workload doesn't depend on external elements to make it work. It needs to be available to execute the right task based on the business need.

All workloads aren't created equal — they come in all shapes and sizes. Despite this difference, they have some common characteristics:

- A workload shouldn't have dependencies (a related piece of code or application that resides in another place within a system).
- The workload should have a consistent interface or Applications Programming Interface (API) so there's a way to connect it to other applications and services.
- A workload must have rules or policies about how it can be used under what circumstances. There may be a policy that states that a set of workloads must be executed in a specific order or at a specific time of year.

Three types of workloads are most frequently managed in the hybrid environment: a batch workload, an analytics workload, and a transactional workload.

The batch workload

Batch workloads are designed to operate in the background. Typical batch workloads include billing applications, fulfillment applications, and complex queries. These workloads require considerable compute and storage resources. Batch workloads are rarely time sensitive and can be scheduled when few real-time tasks are running.

The analytics workload

A growing need exists to analyze information across a network of data sources within a hybrid environment. In an *analytics workload,* an emphasis is placed on the ability to holistically analyze the data embedded in these workloads across public websites, private clouds, and the data warehouse. These types of analytic workloads tend to require much more real-time computing capability.

Transactional workloads

Transactional workloads are the automation of business processes such as billing and order processing. Traditionally

transactional workloads were restricted to a single system. However, with the increasing use of electronic commerce that reaches across partners and suppliers, transactional workloads have to be managed across various partners' computing environments. Therefore, there's a need to focus on business process of these transactional workloads. These workloads are both compute and storage intensive.

Putting Virtualization In Context

Virtualization may seem like a silver bullet to many organizations. After all, with virtualization you can get better utilization of servers. In the good old days, simply adding more servers seemed easier than trying to optimize the data center. However, as data center sprawl becomes more of a financial burden, virtualization became a way to get rid of underutilized servers that took up a lot of room in the data center and used too much power. But over time, as IT management became comfortable with virtualization in the data center; virtualization was more than simply making an individual server more efficient.

Over time, everything seems to be getting virtualized — everything from the hardware platform, the operating system, the network, memory, storage, application, and the desktop. While this process was initially undertaken to make better use of the hardware, virtualization has now emerged as a best practice for enabling cloud computing.

Managing Virtualization

If you recall in Chapter 1, we explained that virtualization is important to the cloud because it decouples the software from the hardware. In cloud computing, you're now dealing with pools of resources rather than individual systems. Does that mean that everything is floating in space (unfortunately, not)? It does mean that the capability stored in physical devices has to be able to act as though each of those capabilities wasn't constrained by where it lives.

While the idea of having these free roaming pools of capability, such as memory, storage, hardware, applications, and so on, is wonderful, they come with a price. Those virtualized

pools of resources have to be managed or they quickly get out of control. What do we mean? Here is an example.

An IT data center manager decided to implement server virtualization to modernize and streamline the data center. Through this type of virtualization, the company reduced the number of servers by a third. At the same time, it stopped the physical expansion of the data center and reduced power consumption by 30 percent. But something started to happen after virtualization was widely implemented. Users began to really like the freedom of virtualization.

When developers initiated a new project, they simply created a new image or copy of the resources they needed. While searching for an existing copy of those resources was possible, it was a lot of trouble, so developers just created new copies. Soon, IT management noticed that things were getting out of control. Developers complained that they didn't have enough memory or storage to complete their tasks. IT complained that they had lost control over who was using resources for which projects. Making matter worse, the Chief Security Officer of the company called a meeting because there were some unexplained intrusions into mission critical systems that could be traced to one of these virtualized images.

This example clearly shows that virtualization without management is a recipe for disaster. This disaster will only grow more critical with cloud computing where virtualization is often the foundation underneath the pools of resources used in public, private, and hybrid clouds.

The solution to managing virtualization effectively is to provide a mechanism for tracking where all resources are physically located and how each of these resources can be effectively and safely used. The overall system has to understand the relationships between elements and the rules for usage.

The following list provides some of the management issues to be considered:

- **If developers want to use an image, management environment should provide rules for proper usage.** Is this developer allowed to create a new image or copy? If not, can that developer use an image created by IT management based on the task?

- **Provisioning the right resources for the right reasons is critical in this type of virtualized environment.** While the images may come from a pool of resources in the private cloud, using outside resources is practical. Public cloud resources are often used in context with a data center or a private cloud to support customer demands. Using compute resources from a public cloud for a pilot project or a new initiative may be more cost effective. Management needs to have the ability to determine how and when these public resources can be used. Implementing these rules in a management system improves governance and helps control costs and security.
- **A security capability needs to be tied to each image that exists in the virtualized environment.** Who's allowed to access this image? When the master image is updated, will this introduce security risks when that image is propagated across the environment? When that image is no longer in use, it should be automatically deleted. Unused but undeleted images can open a security hole. They also take up resources unnecessarily.
- **Performance of the collection of virtualized resources has to be managed.** Remember, with virtualization at every level of the computing, pools of resources have to be managed as if they were a single system. Loads of resources have to be balanced, provisioned based on business rules, and the collection of resources, as a whole, needs to be monitored.

Service management in the hybrid world

Service management is at the heart of management in the cloud. If you look at all the components of services in the data center, the private cloud, and the public cloud, you have a management imperative.

There's tremendous power in transforming computing from a set of disconnected silos into a pool of hardware, software, and networking resources that support the end users. This approach requires that these resources be well balanced, well secured, and well managed so they work as a system.

Chapter 4

Locking Down Security and Governance

In This Chapter

- Making sense of security risks
- Manufacturing a secure private cloud
- Understanding security best practices for the hybrid environment
- Discovering risk and maintaining your cloud security strategy

One of the biggest issues facing companies considering cloud computing is the concern about security and governance. Will cloud computing be as secure as the data center? What happens when business units begin using public cloud services in combination with the data center or a future private cloud? How can you be sure only authorized people are accessing your sensitive data and applications? Is your cloud provider able to provide audit reports to demonstrate your compliance with industry and/or government regulations? These questions are all important. Ironically, a hybrid cloud environment (see Chapter 3 for more information on the hybrid cloud), if implemented in a well-architected manner, can be just as secure and well governed as a traditional data center.

Hybrid environments will be the reality of the future, and your IT governance and security strategy must address the new risks this model entails. In order to ensure that your company's IT resources are safe wherever they're located and whenever they're needed, security must be built right into the fabric of your private cloud.

This chapter presents a foundational best-practices-based approach that can help you think differently about the security and governance of the cloud.

Understanding Security Risks

Organizations have an obligation to ensure the right balance of protection, privacy, governance, and accessibility to key resources — whether in the traditional data center, the private cloud, or the public cloud. Cloud computing requires a delicate balance between the requirement to share resources and the need to protect those resources from unauthorized access, data leakage, and other exposures. It's obvious that you won't want inappropriate individuals to have access to your organization's private data and applications. Therefore, companies providing cloud computing services have alleviated that risk by standardizing and automating processes to protect these shared environments.

Alleviating the risks

Everyone wants to alleviate the risks involved in cloud computing. Basically, you can do this through two processes:

- **Standardization:** Standardization is a consistent and codified process by which a resource is delivered to an application or another resource.
- **Automation:** Automation uses a programming technique to deliver a process in a consistent and repeatable manner.

Using these two processes, only one method of provisioning for each resource is allowed, and only a set number of acceptable ways exist to configure the resources. For example, there may be a rule that says that a developer has to choose from three different options based on the project, the priority of the project, and the security access permitted for that individual. Likewise, if this developer wants to add storage, he's restricted to an amount of storage based on the project requirements. This prevents security breaches based on preventable errors, such as operator error and lack of oversight. These standardized and automated processes provide that oversight without human intervention.

This level of standardization and automation can also lead to cost savings and operating efficiencies inherent in the delivery of cloud services. In turn, this standardization improves the ability of an organization to eliminate errors, meet governance requirements, and maintain service levels.

One of the issues remaining in shared cloud services is the potential risk in implementation. Most companies providing shared services implement multi-tenancy. Multi-tenancy means that each user's code, data, and process are stored in isolated containers. This is the right starting point, but it isn't enough to guarantee a secure and well-governed environment.

On top of multi-tenancy there must be a well-defined set of security services. An infrastructure hosting company, for example, may include intrusion prevention systems and security platforms to provide highly secure cloud environments for its public cloud customers. The company can assure its customers that its data is safe by implementing services designed to anticipate threats and prevent attacks and intrusions from succeeding. The virtualized cloud environment demands specialized software systems that can place a secure container around each customer's data while still providing the benefits of a multi-tenant architecture. Another security benefit providers can offer is real-time monitoring services designed to quickly alert customers about unauthorized activities.

However, this same provider may be asked to demonstrate proper governance of that customers' data. While many hosting providers give some level of operational information to customers, most aren't eager to open up their environment to outside scrutiny. When a company uses public cloud services, it's often concerned by the lack of visibility and uncertainty about performance and availability that comes with relying on a third party for services. Many of these concerns are particularly strong related to issues of change management, workload balancing, and data analysis. However, the cloud provider needs to address the additional security risks that arise because its customer's data is in a shared environment.

When a company uses cloud computing for a highly regulated or mission critical application, the risks inherent in the public cloud may require the company to implement a private cloud. In this situation, the company may select the private cloud over its traditional data center because the application demands the flexibility and self-service of the cloud environment.

The private cloud doesn't eliminate the need to manage security. It puts more of the responsibility for control under the auspices of internal IT staff. In addition, the highly distributed infrastructure of the private cloud means that you need

a dynamic and responsive approach to security instead of the more static and controlled internal IT environment. For example, in the IT environment you're protecting a specifically defined application. In some situations, the cloud environment is used for short-term partnerships or innovative prototypes that are created and changed more frequently.

Combining security requirements for private and public clouds

Most organizations don't have the luxury of only establishing a private cloud where they have complete control. When companies create their private clouds, they typically are required to combine them with some public cloud services, including a Software-as-a-Service (SaaS) offering, some third party computing infrastructure, or storage. While the company doesn't have full control over how the public resources are managed, it can leverage internal security processes and policy to manage public cloud resources.

Assessing private cloud security requirements

A recurring theme across companies planning a cloud security strategy is that requirements vary dramatically depending on their business environment. One size doesn't fit all. You need to begin by understanding the specifics of your environment and then begin to build security into your design.

Make sure that you have the same level of security in your hybrid environments as you have in your traditional environment. So after you've evaluated the industry and organizational requirements you need to construct a secure infrastructure, what are some of the key considerations?

Begin by answering a set of questions that helps you form both your approach to governance and your security strategy. Start by answering the following top questions:

- How do you control access rights? Who has the right to access IT resources? How do you ensure that only the right people gain access to your applications and information?

- How much visibility do you have into the cloud and its operations? How do you monitor, measure, and manage your IT assets across multiple environments?
- Can you implement security policies consistently across all types of cloud architectures?
- How do you protect your data throughout its lifecycle? If your relationship with the cloud provider ends, how can you ensure that your data stored on the cloud is expunged?
- Can you satisfy auditing and reporting requirements for data in the cloud?
- Do you have vulnerabilities in one aspect of your infrastructure that could possibly be repeated many times across your multi-dimensional virtualized environment?
- Do you have a plan to ensure that patches are applied to all images regardless of where they're deployed in the cloud?

Building a Secure Private Cloud

If you read the preceding section, "Assessing private cloud security requirements," you may have the answers in hand that define your IT environment. You're ready to build a secure private cloud. Ensuring that trust and risk management are infused from the beginning requires a good plan in addition to collaboration across all levels of the organization. While the implementation is ongoing and can get very complex, the guidelines in this section can help you get started.

Ensuring data protection

Security of data — whether in a public or private cloud, or data center — is a complex issue that continues to plague the industry. When companies are increasingly distributing their data through customer portals over cloud services, the confidentiality of these data must be maintained. Information governance plays a crucial role in helping you to protect personally identifiable information (PII), such as customer social security numbers, credit card account numbers, or patient health identification numbers.

Your organization needs to develop and publish a consistent set of rules and policies regarding the creation, capture, management, transmission, storage, and deletion of confidential and business critical data. Techniques, such as encryption, should be used to reduce risks, such as data theft and misuse.

Hackers and thieves are always one step ahead of the latest security measure, so data protection tools need to be used in multiple-layers and in a comprehensive and consistent manner. For example, situations exist where thieves have been able to steal encrypted data. In one recent case, the data was encrypted only up to the point the data was delivered to the applications. At that point, it was decrypted and that's when the loss occurred. This loss could've been prevented if the receiving application had been allowed to control the decryption process.

Managing access and identity

Identity management's primary goal is ensuring that authorized users across their enterprise and supply chain have access to the applications, data, and tools that they need, when they need it, while blocking unauthorized access. A standards-based, single sign-on capability is required to simplify user logons for both internally hosted applications and the cloud, allowing users to easily and quickly leverage cloud services. Identity and access management offers tangible, operational benefits of improved user productivity while reducing the risk of security breaches.

And because clouds typically support a large and diverse community, including clients, business partners, and suppliers, identity management has to be implemented in a federated manner — consistently applied and linked across the environment.

One of the weak links in any identity and access management program is the lack of governance around the management of identification credentials and user passwords. For example, many companies create policies for password usage, but don't properly train or document how these rules should be enforced. Sometimes outside contractors are given passwords that don't expire when their work is completed, or an employee may terminate his employment without having his access immediately revoked. Finally, the cloud provider

employs administrators whose identity and access credentials must be managed to ensure those credentials are terminated when appropriate.

Provisioning for secure environments

One of the primary benefits and characteristics of the cloud is its ability to easily provision resources and applications based on need. However, resource provisioning needs to be handled with the right level of control and security.

One of the risks of a highly automated provisioning process is that the number of virtualized images can grow very quickly. If the organization loses control of who created these images, who has access, and who has the authority to make changes, then security may easily be compromised. Unused images must be deleted so they can't be used by an unauthorized user to access information behind the firewall.

All application and virtual image provisioning and de-provisioning activities should be logged and reviewed to ensure that access rules are enforced and audit trails retained.

Controlling governance and audit

Governance is about making good decisions about performance predictability and accountability. Visibility can be especially critical for compliance. Your governance strategy needs to be supported in two key ways:

- You need to understand the compliance and risk measures the business needs to follow.
- You need to understand the performance goals of the business.

Audits are a structured processing of ensuring that companies are following required governmental regulations and best practices. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), European privacy laws, and many other regulations require comprehensive auditing capabilities.

One of the important technical requirements for ensuring compliance with security mandates and producing successful audit reports is the ability to log activity that takes place in the internal data center and private cloud. You need to define when, where, and how to collect log information so you have an automated way to keep track of how well you're doing in terms of managing the confidentiality of your organization's critical and sensitive information.

Dealing with intrusion

Threats can come from a variety of places, and the vulnerabilities are multiplied when you're dealing with hybrid environments. Vulnerabilities across servers, network, infrastructure components, and endpoints need to be assessed and monitored. These threats and vulnerabilities are called *intrusion.* Technology, such as vulnerability scanning, antivirus, intrusion detection, and intrusion protection systems, should be deployed to reduce the threat of malicious software and unwanted intrusion.

Looking into Best Practices for Securing the Hybrid environment

After you have your security measures in place, the IT team can sit back and relax, right? Unfortunately, the answer is no. You need to be constantly aware of changes that may result from innovative business strategies or from a new external threat that hadn't been previously anticipated.

For example, your company may engage a new set of business partners that need access to a specific set of customer and product data that's managed in your private cloud. You need a safe and secure way to provide the new partners with ongoing access to these data. Or you may find that an existing web facing application isn't adequately protected because a previously undetected bug in your application programming interfaces (APIs) has exposed you to intruders.

Being prepared for constant change is one of the most important best practices to follow when securing your hybrid environment. In general, to reduce your security risk in the data center and in public and private clouds, follow these steps:

1. **Authenticate all people accessing the network.**
2. **Implement role-based access control so users have access only to the specific applications and data that they've been granted specific permission to access.**
3. **Remove unnecessary software running on user computers and ensure that all software has a defined business need.**

   This step includes monitoring software or services that are running in the cloud for legitimate business need.

   Your cloud provider needs to automate and authenticate software patches and configuration changes, as well as manage security patches in a proactive way. Why is this so important? Many of the outages experienced by cloud service providers are typically operational errors or configuration mistakes. If a cloud provider doesn't manage software updates and security patches, your information and business services could be at risk.

4. **Ensure all data is encrypted, and that only you and the cloud provider have access to the encryption keys.**

   It's important to protect data while in transit and also while stored in the cloud provider's data center. This is critical to protecting data privacy and complying with security regulations.

5. **Formalize the process of requesting permission to access data or applications.**

   This applies to your own internal systems and the services that require you to put your data into the cloud.

6. **Monitor all network activity, and log all unusual activity.**

   In most cases, deploy intrusion prevention systems (IPS). While your cloud services provider may have a portal that enables you to monitor activities on its environment, you should have an independent view. This is especially important for compliance.

7. **Log all user activity and program activity, and analyze it for unexpected behavior.**

   There needs to be a consistent process for keeping track of activity to meet both security and governance oversight requirements.

Evaluating the Risks and Creating a Cloud Security Strategy

A thorough understanding and evaluation of the risks your company faces is a requirement to creating a sound security strategy. There are different levels of risk, and your company has the responsibility of achieving the level of security that best meets your business requirements, customer expectations, and industry/government regulations, while also keeping cost and resource constraints in mind.

Sometimes these influences may be at odds with each other. In fact, because of these conflicting needs, companies need a governance body representing different interest groups in the organization. This organization is the best method of holistically evaluating risks.

To help you build your security strategy with an understanding of the impact of risk on your decisions, follow these pointers:

- In most circumstances, cloud security needs to be approached from a risk management perspective. If your organization has a risk management team, involve them in cloud security planning.
- IT security monitoring has no simple key performance indicators, but be aware of what similar organizations spend on IT security. That way, you have context for the expected level of investment. Similarly, keep track of time lost due to any kind of attack — a useful measurement of cost that you may be able to reduce over time.

- In a highly distributed environment, managing the identity of who's allowed to access what resources under what circumstances has to be a top priority. Clearly defined rules combined with automation provide a path forward.
- Try to create general awareness of security risks by educating and warning staff members about specific dangers. Complacency is easy, especially if you're using a cloud service provider. However, threats come from within and from outside the organization.
- Regularly have external IT security consultants check your company's IT security policy, IT network, and the policies and practices of all your cloud service providers.
- Determine specific IT security policies for change management and patch management, and make sure that policies are well understood by your service management staff and by your cloud service provider.
- Stay abreast of news about IT security breaches in other companies and the causes of those breaches.
- Review backup and disaster-recovery systems in light of IT security. Apart from anything else, IT security breaches can require complete application recovery.

When a security breach occurs on a specific computer, the applications running on that computer likely need to be stopped and a quarantine implemented to contain the breach. Consequently, security breaches can be the direct causes of service interruptions and can contribute to lower service levels. Also, data theft resulting from a security breach could result in a real or perceived breach of customers' trust in your organization.

Security risks, threats, and breaches can come in so many forms and from so many places that many companies take a comprehensive approach to security management across IT and the business. As your IT environment moves beyond the internal data center to include public and private cloud services, security and governance have to be handled in a cohesive manner based on a coordinated plan.

Chapter 5

Integrating with and within Clouds

In This Chapter

- Defining the need and requirements for cloud integration
- Examining the cloud integration cases
- Maintaining control, security, integrity, and governance

Integrating information and business services across multiple siloed environments is increasingly challenging for many companies. Information needs to be synchronized across multiple data sources that may be managed in your data center, Software as a Service (SaaS) applications, or in your private cloud. Additional complexity arises from the need to use business services across the boundaries of your internal data center and private and public cloud environments. Both the integrity of your information and the ability to incorporate cloud-based business services into your company's overall business processes are at great risk unless you can consistently integrate across your hybrid environment. In this chapter, we describe the requirements for integrating across these platforms.

Understanding the Need for Cloud Integration

Cloud computing can help your company develop the flexibility and agility it needs to bring new and innovative solutions to market quickly and cost effectively. Remember, though, that your journey to the cloud won't follow the same path

for all your workloads (see Chapter 3 for additional info on workloads). Your company has a range of different workload types, such as analytics, business services, collaboration, and development and test. The specific characteristics and requirements of each workload help to determine if it's a good fit for a public or private cloud or if it would be best managed in your internal data center.

In many ways, the need for integration remains the same as it has been for decades — providing the organization with visibility into the transactions, services, and other critical information about the business. Departments, such as finance, operations, human resources, and sales, all typically use applications designed specifically to support their unique business processes. These applications are likely to have unique and independent sources of data.

Regardless of the technical means used to integrate applications across these systems — whether in the data center or in private or public clouds — business and IT must collaborate to ensure accuracy and consistency. To truly innovate, you need a holistic understanding of all the information about your customers, partners, and suppliers.

Make sure your cloud-based information is consistent with information managed in your traditional environment. For example, prior to integrating data across internal data sources, IT may need to account for variability in data definitions, data formats, and data lineage — like a family tree for data.

What's changed? In addition to integrating data across legacy applications in the data center, you may need to integrate data managed in multiple private and public cloud platforms. With business critical data managed in hybrid environments, how does IT recognize which one is the reality? Is your internal legacy system the master or does the truth reside in the application in the cloud? These various systems must be in synch in order for the business to have consistency and predictability within and across its information.

Looking at the Requirements for Cloud Integration

Many companies initially underestimate the challenges of integrating data across hybrid computing environments. They assume they already have the tools and expertise required to manage the integration process because of their prior experiences with integration in the data center.

For example, many companies deploy a service oriented approach to codify business processes into reusable services. This approach lets companies create new services that are consistent, more easily changed, and more easily linked together or integrated. In addition, companies have used Enterprise Application Integration (EAI) to integrate applications within their data centers. EAI technologies have been used successfully to link applications together without the need to make significant changes to the applications.

However, the integration tools used within the data center weren't designed to manage the additional complexities of integrating data and business services across the platforms of the cloud.

Many companies that began with one SaaS application, such as salesforce.com, are quickly moving to rely on multiple SaaS applications as an important segment of its application environment. When companies deploy traditional integration technologies to accommodate these third party environments with information managed in the data center, they often require a lot of work on the part of the IT organization. With enough time and programming staff, companies can create custom coded connections between internal and cloud applications. However, keeping a custom solution up to date can take a lot of ongoing maintenance.

One of the benefits of a SaaS environment is that the developer of that application often makes frequent changes to the structure of the application. Users have automatic access to the most up-to-date version of the software without needing to manage the upgrade process. Users of SaaS services are typically notified of these changes; however, the increased frequency may make it difficult for these users to manage

the integration of the SaaS application with other business services. If, for example, changes in data formats and specifications are made by the SaaS application provider, the company using the service may not be aware of these changes until they experience faults or errors in their own integration processes. In some situations, companies may facilitate the integration process between data in the public cloud and data in internal systems by creating an additional data repository. This causes unwanted delay and complexity.

You need an integration process that's adaptable based on unexpected changes.

To maintain the benefit of using SaaS environments in concert with your line of business applications requires that you establish an effective and repeatable integration process. By leveraging new sets of integration platforms and best practices, you can overcome these integration challenges. Overall, you need a common and standardized way to link your applications wherever they're managed — the four main requirements for creating this standardized approach. These elements are covered in this section.

Connectivity

You need to be able to connect many different types of applications and data — SaaS, custom web, on-premise, and private cloud applications and databases and flat-files — quickly and easily without requiring a lot of ongoing maintenance. You should also consider different types of integration, including data migration, process integration, or some unique new type of integration, including taking data from an internal application, such as SAP, and then displaying these data in a SaaS application.

You may need to make connections between two applications or you may need to connect one application to many application end-points. Even more important will be the ability to scale quickly from a one-to-one integration to a one-to-many integration. In addition, different connectivity protocols or techniques may work better in different situation so you should be prepared to choose different options for different business requirements.

Transformation

In a typical business, you often have to map the data about customers in your line of business application (such as accounting) with data about those same customers in your SaaS application. If you're lucky, the formats of both of these data sources will be the same. However, many times, these applications are designed or managed by completely different groups that never had to communicate with each other. For example, the IT organization manages the data in the ERP system while the sales department has its own staff to manage the data in the SaaS CRM system.

Now, business management needs to ensure that the accounting system is consistent with the sales management system. Your IT staff is most likely familiar with the data format specifications in your legacy applications but doesn't have the same level of understanding of the specifics of the data in your SaaS applications. One of the major advantages of SaaS applications is that business process owners can leverage these applications without any support from IT. All the data management complexity is hidden from the user. But in order to create these necessary mappings, you need to understand, for example, if a customer identification (ID) number is numeric or if it includes alpha characters as well. After you understand the specific characteristics, you can graphically transform the ID number in both applications so they can be recognized and understood as the same information.

Business logic

The systems that have the data you value include business logic and processes that controls the way that data is managed. Therefore, you can't simply connect data elements together without a deep understanding of how these systems behave from a business process perspective. It is helpful, for example, if you can graphically define the flow of data between source and target applications. In this context, you can graphically define all the steps needed to extract purchase order data from your ERP specific system and send it to different system (for example, a specific CRM system). Unless your business is standing still, you can expect to see the SaaS vendor improve the underlying application. It may find a more efficient way to manage a certain business process that impacts how you connect the logic between various systems.

However, the typical SaaS vendor doesn't make arbitrary changes. Most vendors base their approaches to integration on best practices in integration patterns and often reuse these common patterns. By understanding these patterns and watching for changes, your organization is better able to withstand changes in the implementation details.

One way to increase the speed of integration is to use an integration provider who's studied metadata structure of SaaS applications. These vendors can provide a pre-configured integration pattern or template that jump starts the effort of integration between data sources. One of the benefits of working with a standardized template is that the same template can be reused for other integration projects. The template is typically designed to cover about 60 percent of the requirements for a particular integration.

Management

Data doesn't live in isolation. No matter what type of data you're working with, it lives on specific hardware platforms, leverages specific storage environments, and connects with third party services (payment services, credit verification, partner commerce systems, and so on). All these elements become part of the way you manage the flow of data between your applications in the data center and in the cloud.

Therefore, from a management perspective you need to be able to monitor and manage these workloads. The approach you take largely depends on how you manage your business. For example, ask yourself these questions:

- How many third party services do I use?
- Have SaaS applications, such as CRM, Workforce planning services, and the like, become part of my IT strategy?
- Does my business require seamless integration across these business services?
- How much do my business partners and customers depend on the smooth and accurate integration across information sources and business services?

If you don't have a well-planned way to manage these resources and services, the lack of planning can dramatically impact the overall efficiency of your hybrid environment. To be successful in breaking down data and processing silos, you

have to focus on overall management of business workloads. This is especially true because these workloads are becoming increasingly fluid and mobile.

Studying Cloud Integration Cases

As soon as you begin moving workloads into the cloud, you need to establish a way to connect them to existing traditional workloads. While one of the first cloud integration scenarios a company may encounter is the need to integrate traditional resources and services with cloud-based resources and services, most companies very quickly find that they must contend with many different integration scenarios. The three most common cloud integration models are included in this section.

Connectivity to clouds

Connectivity from the data center to the cloud is one of the most basic cloud integration use cases. The typical IT organization manages its ERP system within its data center and uses a SaaS environment to manage sales leads. Sales, order, invoice, and inventory data must be synchronized across these systems for the company to function properly. This can be a major cultural shift for the organization that's used to having full control over its line of business applications.

There is little or no control over the architectural structure of the SaaS environment. Therefore, the IT organization needs to establish new processes to institute management between the data center application and the cloud-based application. IT management needs to separate the data elements within the line of business applications from unnecessary dependencies. For example, there may be a business process that controls a very specific circumstance that interferes with your ability to easily connect between data sources on the cloud.

In addition, there are specific issues related to using cloud computing environments that impact the style of integration. For example, while your company gains huge value from using a SaaS based CRM system, governance requirements demand that customer data be stored behind your firewall. Therefore, when a prospect becomes a customer, the company moves the data into the data center for additional security. This

company now has a hybrid environment to manage. The company needs to automate data mobility across clouds in order to transfer and transform customer data to migrate between public and private clouds.

Connectivity between clouds

Companies may need to integrate between private and public clouds. One common example of this occurs when private cloud resources are insufficient to support peak demand. In this situation, select workloads are allowed to burst into a public cloud environment. For example, an entertainment organization is testing the introduction of a new game that supports on demand group participation. The online gaming community has already shown a great deal of interest surrounding this new introduction. The organization wants to test how its web application scales from 20,000 to 1 million concurrent users before going live. They know they need more cycles and more power than they have available in their private cloud, so they expand their environment by leveraging public cloud resources, such as IBM's Smart Business Development and Test Cloud or Amazon EC2.

Connectivity in clouds

A third key use case occurs when you need to create bidirectional integration with multiple SaaS applications in order to support a business process. In this use case, the connectivity capability itself is in the cloud. For example, a services organization uses sales automation to keep track of its prospects and a different SaaS application to manage commission and salary payments. Many sales situations exist where a cross-brand sales team collaborates in closing a large sales opportunity. As a result, the sales commission must be split across different sales people. The data in the CRM system needs to be consistent with the data in the payment application or the people who worked to close the deal won't get paid accurately.

Automate this process so every time a product is sold you automatically pass the information back and forth to keep track of who made the sales, who owns the account, and who gets the commission. Automating this process requires the synchronization of the data between the two SaaS applications.

Because both of these applications are in the cloud, the most efficient approach to synchronizing the data is to use a cloud-based integration capability. Public cloud offerings include connectivity in the cloud for this type of situation.

Maintaining Governance and Security of Data

One of the top priorities when integrating across multiple cloud environments is that security of information must not be compromised.

The goal of successful integration across public, private, and internal data center environments is to ensure that your company's information is delivered as a trusted resource to customers, partners, suppliers, and employees. In order for this goal to be achieved, your data must be governed according to business and regulatory requirements and secured against unauthorized use and intrusion wherever it resides and is transported. Recognizing these risks, some companies require that all mission critical data remains inside the corporate firewall and, therefore, choose to deploy a private cloud.

However, the proliferation of public cloud and SaaS services means that for many companies there's a lot of uncertainty over exactly where its data resides and if its approach to security can keep up with the increasingly complex security threats.

There are many challenges to maintaining governance and compliance in the cloud and, in fact, we have a whole chapter on security to provide more detail on this topic (Chapter 4). The following sections introduce some of the key governance and security considerations specific to integration are introduced here.

Securing access to data

You need to make sure that security is well designed so that users only are able to access authorized data. For example, there may be different access controls for development versus production teams. Each user should be assigned to a

group based on their privileges ranging from full administrative to project publisher access and read-only access for logs and settings. In addition, certain standard security communication protocols exist that should be followed, such as SSL 128 bit encryption.

Securing the connection

There are several important principals to follow to ensure that the connection between cloud and on-premise applications is secure.

- Data flowing between SaaS applications, on-premise applications, or private cloud applications should be protected by industry standard encryption techniques.
- You need security when you initiate communication between the different platforms to ensure that the integration is safe to proceed.
- You need to ensure that data is not intercepted during the connection.
- The approach to integration you take must help keep order and control — including issues such as software licensing, cost allocation, and charge backs.

When considering a public cloud, you need to understand that you lose control over how many things are done. Use an integration method to monitor these connections and make sure governance standards are met. For example, the SSL/TLS industry standards handshake will help to authenticate using X.509 certificates to ensure that users are legitimate. Part of this handshake process includes creating an encrypted tunnel, some of the security threats this process attempts to protect against are eavesdropping and "man-in-the-middle" attacks. Secure communication protocols exist that should be followed when communicating with endpoint applications and databases.

Chapter 6

Starting Your Cloud Journey

In This Chapter

- Encountering the business imperative of the private cloud
- Outlining the role of IT
- Planning the private cloud

In many situations, a lot of work needs to be done to transform a traditionally siloed computing environment into a flexible and well-managed environment that supports the demands of innovation and business change. In this chapter, you discover how to start planning your private cloud journey. You explore both the issues that you need to take into account as well as the implementation considerations.

Looking into the Business Imperative for the Private Cloud

Business leaders want to be able to use their computing resources to innovate their business in order to identify new revenue opportunities. When a new business strategy is conceived, business leaders may want to quickly experiment and prototype a new online partner-based service without having to wait months for the IT organization to conduct a survey of requirements, purchase new hardware and software to support that initiative, and the like. They want the freedom to use existing resources in new ways without risking capital.

This imperative has led many business leaders to look at public cloud services as an alternative to the data center. However, over time it has become increasingly apparent that business needs the best of both worlds: the flexibility of services on demand with the protection, security, and

governance of the private computing environment. These leaders want assurance that the required service level needed to support business goals will be in place.

Defining the Role of IT

Many IT professionals are concerned about the growing popularity of cloud computing. What's the impact on their jobs? Will a cloud computing environment mean that IT professionals will have little to contribute or manage? It isn't surprising that IT would be concerned about the transition from traditional computing to private and hybrid clouds. However, the reality is that the hybrid world is one vital component in an overall computing strategy.

The private cloud has to be managed in conjunction with both data center services and public cloud services. This transition has actually added important new responsibilities for the IT organization to manage all of these services — the physical environment, the connectivity, the complex data, and the overall service level for the hybrid world. IT will have to manage these key responsibilities:

- **Building shared services based on a service oriented approach:** IT needs to codify and then create well-designed business services with well-defined interfaces. These documented services allow the business to create new applications and services quickly and deploy them in many different situations in the new hybrid world.
- **Consistently manage the synchronization of data center systems of record with data stored in cloud environments:** Data is foundational to an effective hybrid cloud strategy. Data resides in all the key applications and systems that are supported in these environments. Therefore, IT needs to be able to provide effective management of common definitions and rules on an ongoing basis.
- **Managing the overall service level of the combination of all computing services inside and outside the firewall:** While IT management has long focused on meeting service levels within their own data center, the requirements are now expanding with the hybrid cloud. As this evolves, IT will have to incorporate all these public, private, and data center services into a virtual environment

that's managed as though it were a single system through an integrated service delivery approach.

- **Managing configurations, licenses, and the usage requirements for services:** Every environment that becomes part of the hybrid cloud includes system requirements that have to be managed differently. IT has to have deeper control over how configurations relate to each other and how systems coordinate their services.
- **Ongoing support of security and governance:** These issues become more complicated in a hybrid world. IT has to create a security fabric and governance framework that both supports IT and business integrity.
- **Providing cloud integration services between clouds and traditional on-premises applications:** Business units tend to focus on the applications that support their business. IT has a unique opportunity to take a holistic perspective on integration across the extended enterprise.

Considerations when Planning the Private Cloud

Clearly the stakes are high. The private and hybrid cloud environment are important initiatives for both the business and the IT department. But an important initiative like this doesn't happen without significant planning and evaluation. The strategy planning has to be a combined evaluation of both the business strategy and its evolution combined with the technology strategy and how it will evolve to meet business requirements.

This sounds like common sense, but too often business and IT don't collaborate on planning for the future. Successful companies are able to view IT and business as a strategic partnership. Planning for the cloud contains two parts: a set of business considerations and the second is a set of technical considerations.

The most effective approach is actually to involve both IT and business teams in both assessments. This facilitates an understanding of issues and considerations. So what are the key considerations that should be part of the planning and the decision making process? There are five business considerations and five technical implementation considerations.

Business considerations

Business considerations are the strategic goals and plans that determine how the business changes over the next five years. Planning your cloud journey is more successful if it's planned in context with the issues driving the company's strategy.

How is the business changing?

A cloud strategy has to be targeted to how well your organization is structured to support changing business and customer requirements. Therefore, you need to be able to understand the anticipated opportunities and the threats from the competitive environment. Are new competitors entering your market? Is your industry changing so dramatically that it will cause you to totally restructure how you serve customers and partners? If the answers indicate that major change is coming, it will impact the structure and process of creating and managing your hybrid cloud environment.

How does the company want to provide services in the future?

Delivery of services and customer value can transform a company dramatically. Your strategy may be to continue with traditional methods of servicing your customers. However, many industries are finding new channels and new models to support customers. These business models typically depend on sophisticated and emerging technologies. Understanding these requirements helps determine what technologies need to be incorporated into the cloud plan. For example, analytics may play a much far-reaching role than in the past.

What are the financial constraints for the company?

While it's important to understand new business opportunities, it's also important to understand the constraints that the business is experiencing. Therefore, understanding how the business needs to control expenses while increasing productivity and efficiency are essential in the planning for the cloud.

Is the company too siloed for the strategy?

Many business units have acted almost as separate companies — each with its distinctive set of processes, systems, data, and methods of working with customers. However, this approach may be holding the company back from leveraging all assets across the company.

If a company is too siloed, the cloud computing strategy can be structured to help create more cohesion across processes, systems, and data.

Is there an easy mechanism to encourage experimentation and innovation?

It isn't always easy to change your company's culture. However, businesses that are successful make sure that leaders are encouraged to think in creative ways about potential opportunities. Can technology provide a mechanism to support innovation? If this is a business priority, the cloud computing strategy can provide enabling technology to support experimentation.

Implementation considerations

After the business and IT leadership teams have a common understanding of the business drivers, creating a cloud computing strategy will be much more straightforward. Implementation considerations are based on planning for an environment that's based on long-term thinking and creating an environment that's not tied to a single project.

Evaluating reference architectures

A reference architecture is a best practices approach to creating a private cloud based on a composite of successful implementations. Therefore, a reference architecture is a blueprint. While there isn't a single reference architecture, most models have many of the same components. These documents can serve as an excellent planning document.

Focusing on efficiency and flexibility

You don't want to repeat the mistakes of the past. Clouds — whether they're public, private, or hybrid — have to be designed to maximize the ability to standardize and automate. In this way, you have better control over costs and can increase productivity. In addition, this consideration ensures that a standard approach based on best practices is followed consistently.

Planning for a fabric of services

Your environment will incorporate a lot of elements or services that are available across business units. This prepares you to be able to respond across business units as well as with partners. For example, you want consistent fabrics for

managing security, data, integration, and business services. These services should be independent of any specific implementation. Creating this type of best practice establishes a foundation for everything that you create, buy, or connect to.

Assuming that you'll plan for a lightweight approach

Don't over engineer your approach to cloud computing. Make sure that any service or application that is a part of your hybrid environment includes well-defined interfaces (APIs) that are as standardized as possible. You want to have a streamlined approach that allows you to achieve your business goals and support innovation.

Monitoring and managing everything you do

Every service that's created or any service that's used needs to be considered part of your overall cloud environment — even components such as public cloud services (Software as a Service, and so on). You can't just worry about the services you own. Any service that touches an employee, a customer, or partner needs to be monitored and managed with a service level. This approach helps the company better serve its customers, partners, and suppliers in a consistently predictable manner.

Building the foundation for the journey to the cloud

The hybrid cloud environment isn't simply a tactic to improve efficiency in isolation. In reality, it is the path toward transforming information technology into an agent of change. It's a process of moving away from business and technical silos. If a company takes a holistic approach to the cloud computing journey, it can significantly increase the level of collaboration across customers, partners, and suppliers. It can take critical resources that are buried in business units and make them easily accessible assets that support innovation. The journey itself can be a process that supports business change for years to come.