CHAPTER 1

Introduction

This document is written for IT decision makers, architects, engineers, and application owners who make architectural decisions for hybrid deployments. The architecture described in this document is for large and medium-sized businesses that are considering hybrid cloud solutions. This document is also useful for service providers that deliver hybrid cloud services to businesses.

Hybrid Cloud Landscape and Challenges

In December 2012, Cisco commissioned Forrester Consulting to investigate the growing interest in infrastructure as a service (IaaS), and more specifically in the hybrid cloud model. According to Forrester, about half of U.S. and European enterprise IT decision makers report that their companies use cloud IaaS, and Forrester expects enterprises to increasingly adopt IaaS. In many enterprises that are adopting private clouds, on-premises infrastructure cannot always provide the resources needed to address unplanned growth. The hybrid cloud architecture combines private cloud infrastructure with cloud service provider infrastructure to provide users with essentially unlimited resources in the public cloud, with security and control managed in the private cloud.

IT decision makers report that their greatest interest in IaaS in a hybrid cloud is as a complement, rather than a replacement, for on-premises capacity. These decision makers are planning for the resulting impact on network operations and spending. Although a hybrid approach promises cost savings and significant gains in IT and business flexibility, some concerns remain about management and integration of on-premises infrastructure with cloud services in a hybrid cloud architecture.

Forrester asked 69 IT decision makers in the United States, United Kingdom, France, and Germany about their cloud strategies. These decision makers were interested in using, or were already using, a service provider for cloud IaaS. A large majority (76 percent) plan to implement hybrid clouds. In addition, the 2012 Gartner Data Center Summit survey suggests that 70 percent of enterprises will pursue hybrid cloud strategies by 2015. Most hybrid cloud adopters plan to use IaaS as a complement to on-premises servers and storage, but a significant number also look to service providers for peak workload and other use cases.

Forrester also reports that in firms using IaaS, decision makers state that the most valuable benefits of a hybrid cloud strategy are IT flexibility, reduced costs, and faster, more flexible responses to market and business needs. IT decision makers are also clear about their views of the potential challenges associated with a hybrid cloud strategy. Many want consistent security policies and highly secure communications that span the data center and the cloud service provider, and they want to learn how to make existing applications work in both locations. Other important needs include transparent integration with cloud service providers for movement of virtual machines, shared networks with cloud service providers, and consistent application management across the hybrid cloud architecture.

IT decision makers will seek solutions to these challenges using existing tools and skills, or they will explore new offerings that make it easier to address the challenges of hybrid cloud strategies. Evolving solutions that address the most immediate hybrid cloud challenges include:

- Consistent policy enforcement and capabilities for firewalls, security, and application delivery
- Highly secure network connectivity for virtual machine migration
- A common view of workloads and resources across data centers and cloud service providers
- Support for heterogeneous hypervisor environments and infrastructure software
- Workload mobility and portability

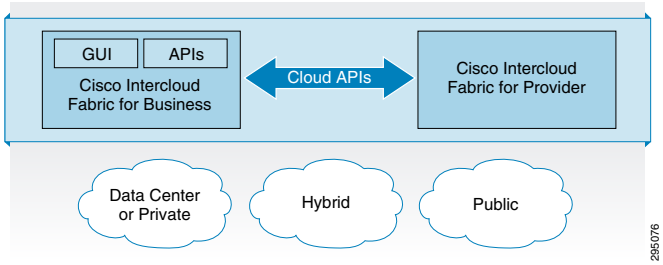
Cisco Intercloud Fabric Overview and Value Proposition

Cisco Intercloud Fabric is a software solution that enables customers to manage and access their workloads across multiple public clouds in a heterogeneous environments, giving customers choice and flexibility to place their workloads where it benefits the most and according to a technical (capacity, security, etc.) or business (compliance, etc.) needs.

With Cisco Intercloud Fabric, customers can choose what networks can be securely extended to the public cloud, and consistent network configuration and security policies can be enforced throughout the hybrid cloud. Intercloud Fabric mechanism to enforce security goes beyond the secure tunnel between private and public clouds, and extends the security all the way to the Virtual Machines (VMs) running in the cloud, so the communication between these VMs in the cloud can be secured as well. This mechanism is explained later in this document.

Figure 1-1 illustrates the solution footprint for enterprise customers, where Cisco Intercloud Fabric for Business can be deployed in the private cloud in heterogeneous environments. This software solution gives IT an admin portal that allows management of workloads, security policies, and network extension to the cloud, and includes northbound API capabilities to allow integration with existing private cloud management solutions. IT customers, including enterprise lines of businesses, can take advantage of Intercloud Fabric for Business embedded self-service catalog to create new workloads in multiple clouds, and manage workload lifecycle and migration through its end-user portal.

Figure 1-1 Cisco Intercloud Fabric Solution



Cisco Intercloud Fabric for Provider is a multi-tenant software appliance that is installed and managed by the cloud providers that are part of the Intercloud Fabric ecosystem. This virtual appliance creates Cloud API uniformity across different cloud providers and abstracts the complexity of supporting heterogeneous Cloud APIs. In the future Intercloud Fabric for Provider will help to build Cisco infrastructure-specific differentiation for all Cisco Powered Cloud Providers.

Cisco Intercloud Fabric gives customers multiple choices of cloud providers, including the ecosystem of Cisco Powered Cloud Providers and the hyper scale public clouds such as Amazon EC2 and Microsoft Azure. Cisco believes that business customers also want choices of hypervisors for their virtualized

environment, so it is important for the solution that enables hybrid cloud to be hypervisor agnostic. The scenario with multiple choices of hypervisors on premises and off premises can make workload mobility and portability difficult, but Cisco Intercloud Fabric resolves this problem and makes this transparent for customers, allowing workloads to be moved to multiple clouds and back to the enterprise.

In summary, Cisco Intercloud Fabric aims to provide a more flexible response to business needs and addresses the potential challenges of hybrid clouds, among other benefits that can be described as follow:

- Workload security throughout the resulting hybrid clouds.
- Consistent operations and workload portability across clouds. Cisco Intercloud Fabric delivers unified hybrid cloud management for end users and IT administrators, enabling workload mobility to and from service provider clouds for physical and virtual workloads.
- To protect critical business assets and meet compliance requirements, Cisco Intercloud Fabric provides highly secure, scalable connectivity to extend private clouds to service provider clouds.

Cisco Intercloud Fabric Use Cases

Cisco's industry research shows that the most common use cases for hybrid cloud designs are development and testing, capacity augmentation, and shadow (rogue) IT control. The Cisco Intercloud Fabric roadmap adds support for disaster recovery.

Development and Testing

In the development and testing use case, enterprise customers develop workloads in service provider clouds and bring the workload back to their private clouds after the workload is promoted to the production environment. To achieve the economic benefits of the cloud and support faster development, many application developers use service provider clouds for the development and testing environment.

However, deployment of production applications in service provider clouds raises critical security and compliance concerns for IT departments. IT decision makers want to provide flexibility to application developers and enable them to use cloud service providers, but they require production workloads to be deployed in private clouds with security and controls to meet compliance requirements such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley mandates. Cisco Intercloud Fabric provides this flexibility with its capability both to move workloads into service provider clouds and to bring workloads back into the customers' private clouds and on-premises infrastructure.

Capacity Augmentation

The capacity augmentation use case addresses the need for temporary resources. For example, to meet seasonal demands, an enterprise can rely on the service provider cloud to provide temporary resources; when high-demand processing finishes, the resources are decommissioned. For example, during peak shopping seasons for retailers or tax season for financial services, there are planned and unplanned demands for additional cloud resources for short and long durations. To achieve the economic benefits of a hybrid cloud, customers can flexibly extend to service provider clouds to meet peak demands while benefiting from the security and control of the private cloud. The Cisco Intercloud Fabric solution transparently delivers required capacity while providing the security and control of a private cloud.

Shadow IT Control

Many enterprises prefer to deploy development workloads in the public cloud, primarily for convenience and faster deployment. This approach can cause concern for IT administrators, who must control the flow of IT traffic and spending and help ensure the security of data and intellectual property. Without the proper controls, data and intellectual property can escape this oversight. The Cisco Intercloud Fabric solution helps control this shadow IT, discovering resources deployed in the public cloud outside IT control (Appendix A, "Shadow IT and Cisco Cloud Consumption Professional Services") and placing these resources under Cisco Intercloud Fabric control.

Intercloud Fabric Deployment Models

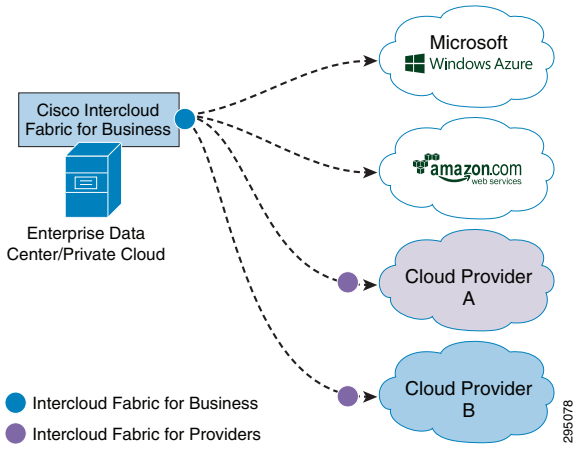
Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed and Service Provider Managed.

Enterprise Managed

In the enterprise managed hybrid cloud deployment model, an enterprise manages its own cloud environments. Cisco Intercloud Fabric uses hybrid cloud scenarios, extending the private cloud into a public cloud while granting administrative control over both the private and public clouds to the enterprise IT department.

In this hybrid cloud scenario, an enterprise contracts with a service provider, and the service provider provides some cloud resources (computing, storage, and network connectivity) for use by the enterprise. The enterprise, by using the Cisco Intercloud Fabric solution, then transparently and securely extends its network into the public cloud, allowing those resources in the public cloud to be treated and handled just as if they were in the on-premises private cloud. All security and policy requirements are applied across the entire hybrid cloud (Figure 1-2).

Figure 1-2 Enterprise Managed Hybrid Cloud



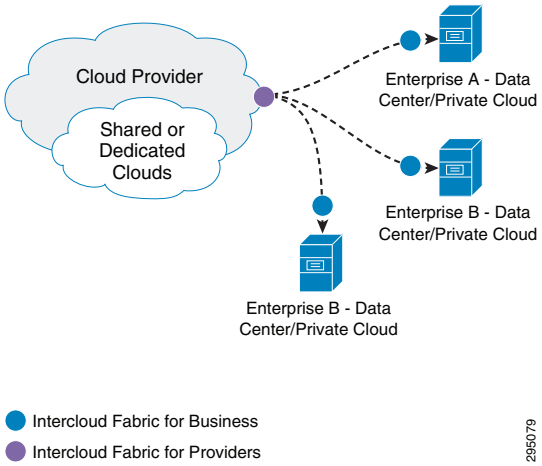
Service Provider Managed

In the service provider managed hybrid cloud scenario, the service provider administers and controls all cloud resources. Customers of the service provider use those resources and deploy their workloads on the service provider managed cloud, but the service provider retains administrative control over the entire cloud environment.

This scenario allows customers to focus on bringing new applications and technology to the marketplace faster, without having to focus on running the data center.

This scenario still allows the creation and use of hybrid clouds. Cisco Intercloud Fabric provides transparent and highly secure connectivity between both private cloud environments (typically called virtual private clouds [VPCs]) and a variety of public clouds (Figure 1-3).

Figure 1-3 Service Provider Managed Hybrid Cloud



Greenfield Deployment

The Cisco Intercloud Fabric solution can greatly benefit organizations that are in the early stages of adopting the public cloud but have not yet taken that step. The Cisco Intercloud Fabric solution can more securely manage workload migration between private and public clouds and support cross-cloud policy consistency.

Brownfield Deployment

Organizations in which developers have already circumvented IT and deployed public cloud solutions can use Cisco Cloud Consumption services (Appendix A, “Shadow IT and Cisco Cloud Consumption Professional Services”) to identify public cloud use and restore cooperation between IT and developers. Such organizations can consider the following approach:

- Use Cisco Cloud Onboarding services to migrate workloads to a service provider that can meet the organization's compliance requirements. These services provide the benefits of bulk purchasing, bringing all IT costs under a common authority, and meet availability and business-continuity requirements.

- Return the workloads to IT management by deploying Cisco Intercloud Fabric and integrate the solution with the organization's existing infrastructure and tools; this approach supports a simple, highly secure hybrid cloud integration plan.
- Continue using Cisco Cloud Consumption services to track public cloud use.