Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions

Point of View White Paper for U.S. Public Sector

1st Edition

Contents

Executive Summary

Public sector and federal government agencies are looking for better vehicles to tame IT budgets, and at the same time provide agile IT services to organizations, citizens and constituents. The paradigm of cloud computing, which has been recently introduced and developed, offers means for public managers and government executives to address issues of budget constraints and agility of service. Simultaneously, new cloud computing-based business models and vehicles are being debated, defined, and implemented in the industry. If adopted and implemented, these business models would require not only new architectures, but also new ways to acquire and procure IT services. These requirements imply that governments need to carefully evaluate how to adopt cloud computing.

A few companies in the marketplace recognize this market transition, and are prepared with a strategy and solutions to bring this paradigm to reality. Cisco is well positioned to provide public sector and federal government agencies with strategy, architecture, and solutions for cloud computing. Cisco defines cloud computing as a means to deliver IT resources and services in an abstract fashion from underlying components, with traits of at-scale, on-demand and multitenancy. These traits directly contribute to the cost savings (both the operating expenses [OpEx] and the capital expenses [CapEx] sides of the equation) and the flexibility of IT service delivery. Consequently, Cisco's cloud computing strategy and solutions are based directly on these fundament traits.

Cisco takes a collective point of view on cloud computing, and envisions that there will be different types of clouds (public, private, virtual, and inter-clouds), and many different services (software, platform, and infrastructure) would be delivered via the cloud marketplace. Cisco also believes that virtualization and the network will be the underpinnings for all cloud types and architectures. This premise positions Cisco to provide normalization, utilization, and mobility of cloud services in a comprehensive fashion. In the Cisco vision, there would be a vibrant marketplace of clouds in the not-too-distant future. Cisco also realizes that one of its eventual goals is to provide federation and interoperability via network enablement among several marketplace clouds.

Cisco brings key frameworks and unified technology building blocks, which will initially enable adoption of cloud computing internally to an IT organization, via private cloud data centers. These private cloud data centers would eventually extend externally to acquire and expand IT services. Cisco's next-generation cloud data architecture is based on a unique, unified, and integrated approach, which addresses these specific facets of cloud computing. Moreover, Cisco clearly understands the challenges in adoption of cloud computing, namely issues of trust, security, standardization, and ecosystems. Thus Cisco brings not only concepts and technologies, but also key standards and partnerships to tackle these challenges. Finally, Cisco provides a coordinated approach, from both a technology and an IT strategy point of view, to adopting cloud computing.

This paper seeks to help in the above process. It provides a high-level overview of cloud computing, outlines some of its key benefits, reviews frameworks and data center technologies developed by Cisco, looks at some of the most important challenges of cloud computing, and finally, suggests some early steps that can be taken toward its adoption.

Introduction

This paper will discuss the strategy, architecture, and solution details that Cisco brings to the industry and governments. For the purposes of this paper, we will focus on the data center aspects of cloud computing. The intended audience for this paper includes public managers, government executives, IT decision makers, and IT professionals who are evaluating cloud computing strategy and cloud data center solutions.

Cloud computing is changing the way that IT resources are utilized and consumed. Public sector and federal government entities want the ability to access infrastructure how and when they choose. IT teams are being asked to accommodate this shift in the consumption model and explore initial use cases. Although the field is in its infancy, the model is taking the IT world by storm. It is clearly the direction that governments are adopting to be more agile and

efficient. Cloud computing can be provided using an enterprise's data center, or by a cloud provider or a government cloud.

If we review the legacy of computing and data centers, we can see an interesting phenomenon currently in the marketplace. Data center computing began with the mainframe in the 1960s, which gave way to minicomputers; both were aggregated models of data center computing. This phase was followed by the distributed computing model of client/server computing, and subsequently the emergence of the Internet and web. Until recently, history has witnessed a market with compromises between scale and complexity. These compromises are addressed, with the emergence of virtualization, which is a disrupting force because it enables abstraction of services and applications from the underlying IT infrastructure. Virtualization within the network is the foundation of the evolution of cloud computing architecture.

Cisco has the vision, strategy, and solutions to become the preeminent provider of infrastructure to the upcoming cloud computing market.

Cisco Definition of Cloud Computing

Cisco defines cloud computing as follows:

IT resources and services that are abstracted from the underlying infrastructure and provided "on-demand" and "at scale" in a multitenant environment.

The Cisco definition of cloud computing is general; however, three key attributes of the definition include:

- "On-demand" means that resources can be provisioned immediately when needed, released when no longer required, and billed only when used.
- "At-scale" means the service provides the illusion of infinite resource availability in order to meet whatever demands are made of it.
- "Multitenant environment" means that the resources are provided to many consumers from a single implementation, saving the provider significant costs.

In the Cisco point of view, all three attributes are required to be considered as a cloud service. One interesting point to note is that the physical location of resources (On-premise or off-premise) is not a part of the definition.

Benefits of the Cloud

Cloud computing fundamentally changes the way that IT services are delivered to organizations. Instead of both owning and managing IT services for themselves, or using an outsourcing approach built around dedicated hardware, software, and support services, organizations can use cloud computing to meet their IT requirements using a flexible, on-demand, and rapidly scalable model that requires neither ownership on their part, nor provision of dedicated resources.

Some of the benefits that cloud computing brings are as follows:

Reduced Cost: Cost is a clear benefit of cloud computing, both in terms of CapEx and OpEx. The reduction in CapEx is obvious because an organization can spend in increments of required capacity and does not need to build infrastructure for maximum (or burst) capacity. For most enterprises, OpEx constitutes the majority of spending; therefore, by utilizing a cloud provider or adopting cloud paradigms internally, organizations can save operational and maintenance budgets.

Flexibility: Flexibility benefits derive from rapid provisioning of new capacity and rapid relocation or migration of workloads. In public sector settings, cloud computing provides agility in terms of procurement and acquisition process and timelines.

Improved Automation: Cloud computing is based on the premise that services can not only be provisioned, but also de-provisioned in a highly automated fashion. This specific attribute offers significant efficiencies to enterprises.

Focus on Core Competency: Government agencies can reap the benefits of cloud computing in order to focus on its core mission and core objectives and leverage IT resources as a means to provide services to citizens.

Sustainability: The poor energy efficiency of most existing data centers, due to poor design or poor asset utilization, is now understood to be environmentally and economically unsustainable. Through leveraging economies of scale and the capacity to manage assets more efficiently, cloud computing consumes far less energy and other resources than a traditional IT data center.

Architectural Considerations

Cloud Computing Infrastructure Model

Government agencies need to consider several infrastructural models when evaluating cloud-computing architecture. Cisco sees four categories of cloud currently in the marketplace or emerging in the near future: public clouds, private clouds, virtual private clouds, and eventually inter-clouds.

Public Clouds

Public clouds are “stand-alone,” or proprietary, clouds mostly off-premise, run by third party companies such as Google, Amazon, Microsoft, and others. Public clouds are hosted off customer premises and usually mix applications (transparently) from different consumers on shared infrastructure.

Private Clouds

Private clouds are typically designed and managed by an IT department within an organization. A private cloud is usually built specifically to provide services internally to an organization. Private clouds may be in a collocated facility or in an existing data center. This model gives a high level of control over the cloud services and the cloud infrastructure. Cisco has a strong portfolio of solutions, products, and services, which enable private cloud infrastructures.

Virtual Private Clouds

Virtual private clouds allow service providers to offer unique services to private cloud users. These services allow customers to consume infrastructure services as part of their private clouds. The ability to augment a private cloud, with on-demand and at-scale characteristics, is typical of a virtual private cloud infrastructure. Private cloud customers can seamlessly extend the trust boundaries (security, control, service-level management, and compliance) to include virtual private clouds.

The virtual private cloud concept introduces the complexities of migrating workloads and related data from a private cloud. Cisco is already developing a unique set of capabilities in the form of protocols and solutions, which enable long-distance, workload mobility scenarios from private clouds to virtual private clouds.

Inter-cloud

Cisco envisions, that in long term, the inter-cloud will emerge as a public, open, and decoupled cloud-computing internetwork, much like the Internet. In a sense, the inter-cloud would be an enhancement and extension of the Internet itself. Just as the Internet decouples clients from content (i.e., you don’t have to have a preexisting agreement with a content provider to find and access its website in real time), the inter-cloud will decouple resource consumers (enterprises) from cloud resource providers, allowing the enterprises to find resources on demand with providers. Workload migration will be the dominant use case for the inter-cloud, as an open market, establishes trust standards and public subsystems for naming, discovering, and addressing portability and data/workload exchange.

Cisco is already working on such an effort in the form of standards, protocols, and partner ecosystems to realize this vision of an inter-cloud.

Service Layers of Cloud Computing

The Cisco view of cloud computing is all encompassing, in terms of the architectural stack in a typical service value chain. These are services that are offered in a traditional IT data center. In a cloud value chain, they are virtualized and delivered on demand.

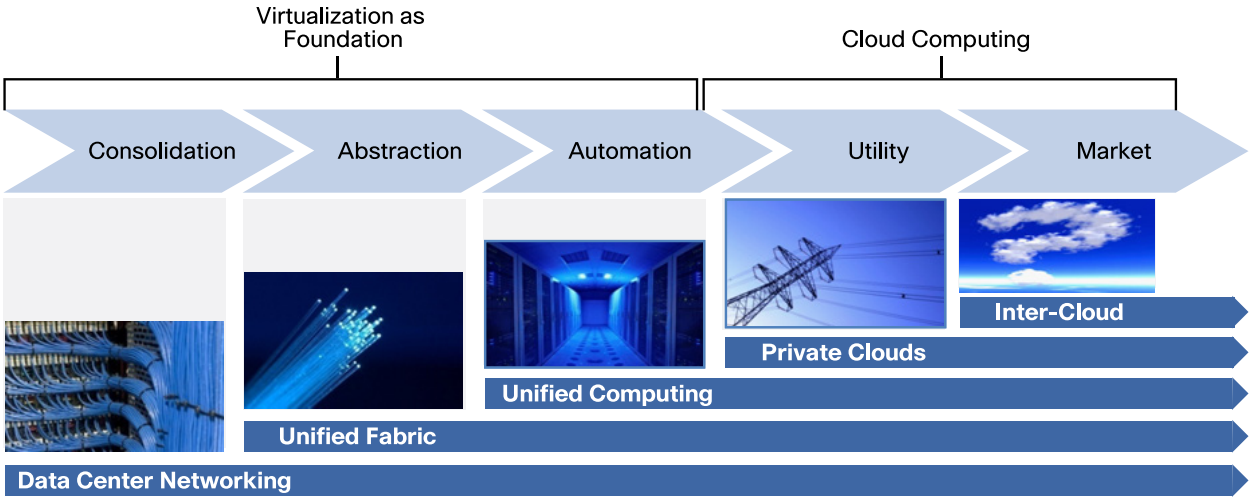
The four major layers in the cloud computing value chain are as follows:

- **Software as a Service (SaaS)** is where application services are delivered over the network on a subscription and on-demand basis. Cisco WebEx™, Salesforce, Microsoft, and Google are a few providers in this layer.
- **Platform as a Service (PaaS)** consists of run-time environments and software development frameworks and components delivered over the network on a pay-as-you-go basis. PaaS offerings are typically presented as API to consumers. Examples of this are: Google Apps Engine, Amazon Web Services, force.com, and Cisco® WebEx Connect.
- **Infrastructure as a Service (IaaS)** is where compute, network, and storage are delivered over the network on a pay-as-you-go basis. Amazon pioneered this with AWS (Amazon Web Service), and now IBM and HP are entrants here also. The approach that Cisco is taking is to enable service providers to move into this area.
- **IT foundation** is the basis of the above value chain layers. It provides basic building blocks to architect and enable the above layers. Cisco partners with several industry players to provide this foundation.

Cisco is an enabler of the Infrastructure as a Service Layer and provides specific services in the Software and Platform as a Service Layers. Additionally, Cisco will provide specific and targeted SaaS and PaaS offerings, like Cisco WebEx.

Cisco Cloud Data Center Evolution Path

Figure 1. Cisco Cloud Data Center Evolution Roadmap



Cloud computing is a natural extension of the Cisco data center strategy. Cisco has developed a roadmap of how cloud data centers will evolve from the current state to an eventual future state, Figure 1. In this multiphase roadmap, Cisco walks through key cloud infrastructure evolution phases and architectural enablers that Cisco brings to the enterprises and the cloud computing industry. The first few initial phases are based on the constructs of pervasive virtualization, and the final phases show cloud computing evolution.

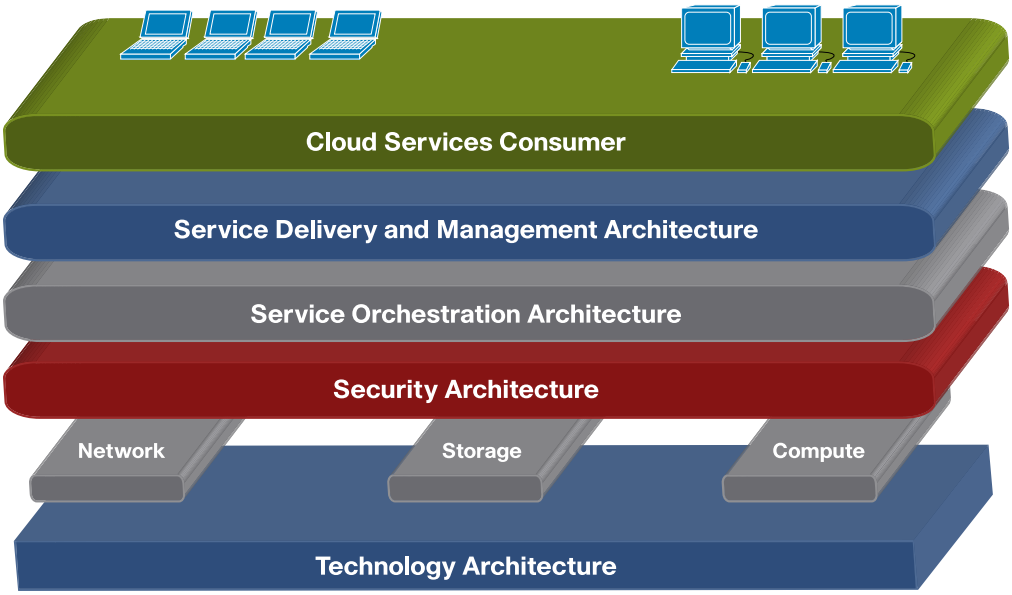
- The first evolution phase is consolidation and aggregation of assets in a data center. This phase regains control on distributed data center assets. The enabling architecture here is data center networking, where Cisco has traditionally been a leader. This phase lays the foundation for data center cost containment and increased utilization through standardization of building blocks.
- The second phase of cloud data center evolution is abstraction. This is a key phase because the data center assets are abstracted from the services that it actually provides. Virtualization technologies enable the abstraction and hence pooling of resources to be shared across the organizations. Data centers are designed around virtual machines, which are the new atomic units of computing. Cisco brings a similar architectural innovation to this phase called “unified fabrics.” This architectural enabler virtualizes different types of networks (LAN, SAN, and IPC) into one single unified fabric. The basis of this phase optimizes and extends data center technologies through virtualization across the network, storage, and servers.
- The third phase of the cloud data center evolution is automation. This phase capitalizes on the consolidated and virtual aspects and provisions services in a rapid and automated fashion. The fundamental architectural building block that Cisco brings to the table is “unified computing.” This phase moves beyond cost savings and simplified data center management to improve business agility through technology integration. Unified computing virtualizes the entire data center through a pre-integrated architecture that brings together network, server, and compute virtualization.
- The fourth phase is the enterprise class cloud. This phase starts turning the cloud computing concepts to actionable reality. With the foundation of previous phases, IT services are delivered in the form of a utility. With unified fabric and unified computing as the architectural basis, enterprises and service providers can now start building private and public clouds.
- The final and eventual phase in the roadmap is the intercloud. This phase marks Cisco’s long-term vision of this market transition, marked by ubiquitous, portable workloads and a rich cloud environment, in which many external and internal clouds will coexist, federate, and share resources dynamically. This dynamic marketplace will extend enterprises to providers and providers to providers, transparently, securely, and seamlessly, based on available capacity, power cost, and proximity, and will drive a new wave of innovation and investment similar to what we last saw with the Internet explosion of the mid-1990s.

Cisco’s Solutions to Enable Cloud Data Centers

As part of the cloud data center build-outs, Cisco is bringing some key frameworks, architecture, and building blocks to the industry.

Cisco Cloud Reference Architecture Framework

Figure 2. Cisco Cloud Reference Architecture Framework



Cisco has developed the depiction, shown in Figure 2, of a cloud reference architecture model, which portrays the architectural layers, connected via APIs and repositories. If we study the framework more closely, the following aspects can be articulated. At the foundation of this framework is the data center technology architecture, which consists of three salient blocks of network, compute, and storage. This layer hosts all the services that are delivered to a cloud consumer or subscriber. This layer will be discussed in more detail in later sections of this paper. The next important layer is the security layer. The key takeaway in this layer is that security is blanketed as an end-to-end architecture across all aspects of the framework. Security is considered as one of the key challenges to be solved in a cloud framework; hence, it has to be accounted for in a comprehensive sense. This layer will be discussed in more detail in later sections of this paper. Following the technology and security layer is the Service Orchestration layer, which is implemented with configuration repository enablers. The configuration repository stores key information such as service catalogue, asset inventory, and resource-to-service mappings. This layer is an important layer because it maps the technology components to the service components and serves as a reference point during service provisioning. The service orchestration layer is the “glue” that integrates the lower layers to create a service for delivery. The next layer is also where infrastructure and service management function take place. The topmost layer is the consumer-facing layer, usually exposed via a portal-like solution. This is the layer where service is defined, requested, and managed by the consumer.

Let’s walk through a use case scenario where this framework is utilized.

1. Consumer logs on to a cloud portal and verifies/updates credentials and information.
2. Based on the consumer entitlement, a selected a set of services are identified and presented for definition.
3. The end user selects the service for consumptions and triggers a service-provisioning request.
4. Resources are marked as reserved for service, and a new request is created for services provisioning.
5. The individual domains of compute, network, and storage are configured and provisioned, with requested security and service-level agreements (SLAs), for service delivery.

Hence, this framework provides a working structure to create, define, orchestrate, and delivery IT service via a cloud. Cisco provides not only this framework, but also key solutions to deliver cloud services.

Cisco Cloud Data Center Building Blocks

Cisco brings an important set of technology building blocks at the foundation of the cloud architectures. They are described as follows.

10 Gigabit Ethernet

A cloud data center is designed with the high density of virtual machines coupled with a high processor core count. From a networking perspective, the increase in virtual machine and processor core density promotes a transition to 10 Gigabit Ethernet as the required mechanism for attaching servers. Multiple virtual machines on a single server can quickly overwhelm a single Gigabit Ethernet link, and multiple Gigabit Ethernet links can increase costs. Moreover, there needs to be a strategy in place to not only take the existing investment in 1 Gigabit Ethernet and seamlessly integrate it into a 10 Gigabit infrastructure, but to also enable migration to 10 Gigabit Ethernet and unified fabric (described next). Interestingly, this adoption necessitates virtual machine–aware networking. Cisco is bringing new terminology and implementation to the industry in this regards, called VN-Link. VN-Link is the virtual link between the virtual machine and the physical interface of the physical server. This implementation will enable operational consistency down to the individual virtual machine as well as policy portability, so network and security policy follows virtual machines as they move around the data center. Cisco VN-Link helps enable new capabilities and features, simplifies management and operations, and allows scaling for server virtualization solutions. Specific benefits include:

- Real-time policy-based configuration
- Mobile security and network policy, moving policy with the virtual machine during virtual machine mobility, and live migration for persistent network, security, and storage compliance
- Nondisruptive management model, aligning management and operations environments for virtual machines and physical server connectivity in the data center

Unified Fabric

If one studies a typical data center server infrastructure, it is easy to notice that servers have a series of network interfaces connected to multiple types of networks (LAN, SAN, IPC). This arrangement adds complexity in the form of cost, cabling, port count, scalability, power, and cooling. If we follow the same tradition in a cloud data center, this architecture will not scale to the density that is typically expected. Hence, to continue to reduce the total cost of ownership (TCO) and to deploy virtual machines, all servers must have a consistent and ubiquitous set of network and storage capabilities. One of the simplest and most efficient ways to deliver these capabilities is to deploy a unified fabric. The shift to a unified fabric gives all servers (physical and virtual) access to the LAN, SAN, and IPC networks, allowing more to be consolidated in the customer's network for greater efficiency and costs savings.

Cisco is offering not only 10 Gigabit Ethernet, but also lossless 10 Gigabit Ethernet, currently called Data Center Ethernet or Enhanced Ethernet. This becomes the foundation to consolidate fabrics like Fiber Channel (for SAN), which require the stringent lossless nature of a network. Fibre Channel over Ethernet (FCoE), which is a standard accepted by standard bodies and industry, is leading the way to unify fabric on a cloud data center. Hence, to consolidate server I/O, the server access layer must be adapted to support a unified fabric. Additionally, a new breed of adapters, called converged network adapters (CNAs), would be implemented in the server platform, which will act at the consolidation and virtualization point in the compute layer.

Unified Computing

The unified fabric now enables a fully virtualized cloud data center with pools of computing, network, and storage resources, through the Cisco Unified Computing System (UCS).

The Cisco UCS bridges the silos in the classic data center, enabling better utilization of infrastructure in a fully virtualized environment, and creates a unified architecture using industry-standard technologies that provide interoperability and investment protection. UCS unites computing, network, storage access, and virtualization

resources into a scalable, modular design that is managed as a single energy-efficient system. This system is managed through an embedded management framework, in the Cisco UCS platform.

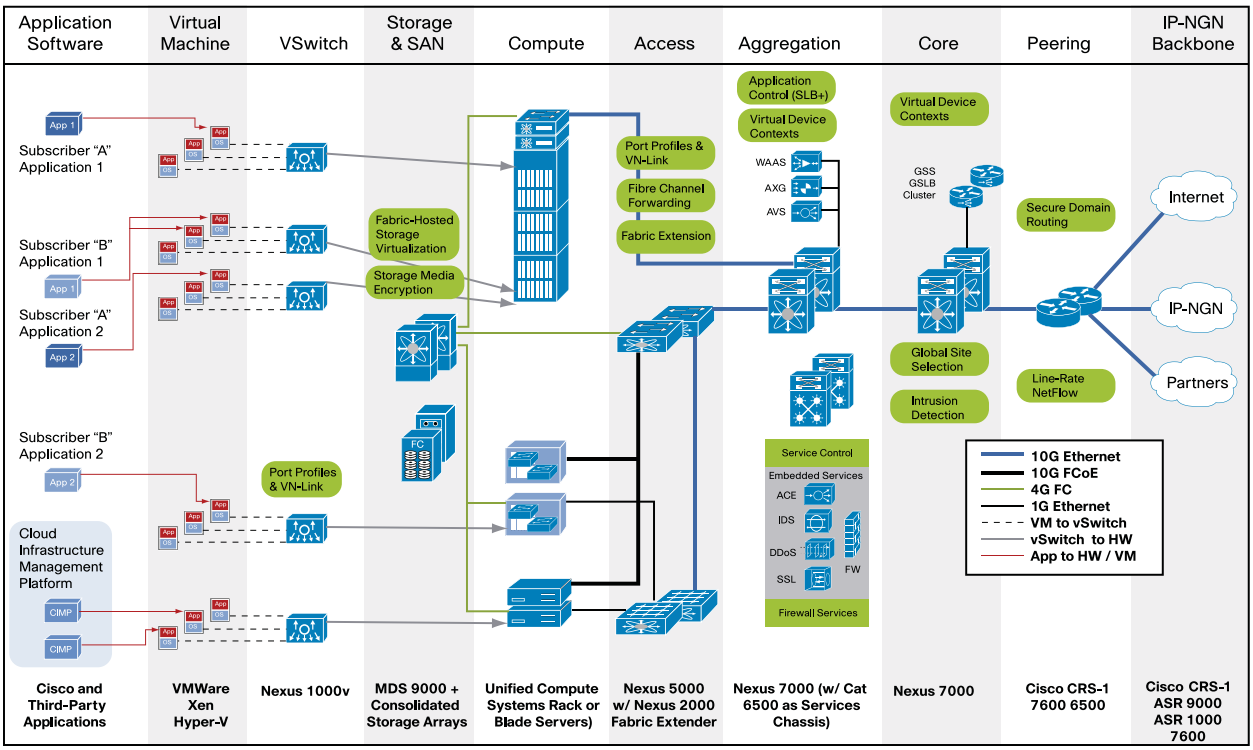
The Cisco UCS management framework provides robust API for managing all system configuration and operation. Its also helps increase cloud data center staff productivity, enabling better management of storage, networking, computing, and applications to collaborate on defining service profiles for applications. Service profiles help automate provisioning, allowing cloud data center to provision applications in minutes instead of days. This provides a means to stateless computing, where compute nodes have no inherent state pertaining to the application that it might execute. So, at any given time, a machine could be running operating systems X, and then the next minute, it could be rebooted and it could be running a Hypervisor Y. Hence, the compute node is just an execution engine with CPU, memory, disk, flash, or hard drive. The core concept of a stateless computing model is to separate the access to the application from the execution of the application. Stateless computing provides a holistic way to address configuration management, rapid provisioning, upgrades/downgrades, scalability, policy enforcement, and auditing.

Cisco UCS provides support for a unified fabric over a low-latency, lossless, 10-Gbps Ethernet foundation. This network foundation consolidates today's separate networks: LANs, SANs, and high-performance computing networks. Network consolidation lowers costs by reducing the number of network adapters, switches, and cables and thus decreasing power and cooling requirements. Cisco UCS also allows consolidated access to both SANs and network attached storage (NAS). With its unified fabric, the Cisco UCS can access storage over Ethernet, Fibre Channel, FCoE, and iSCSI, providing enterprises with choices and investment protection. In addition, storage access policies can be preassigned for system connectivity to storage resources, simplifying storage connectivity and management. The new Cisco UCS platform is, based on the Intel Xeon processor families, offer patented extended memory technology to support applications with large data sets and allow significantly more virtual machines per server, a key requirement for Cloud Data Center and Applications. Cisco UCS network adapters include adapters optimized for virtualization, compatibility with existing driver stacks, and efficient, high-performance Ethernet. With integrated management and "wire-once" unified fabric with the industry-standard computing platform, the Cisco UCS optimizes virtualization, provides dynamic resource provisioning for increased agility, and reduces total overall data center costs, in CapEx and OpEx.

Offering a new style of dynamic IT, Cisco UCS extends virtualized data centers and creates a foundation for private clouds that federate with compatible virtual private clouds. With the virtualized environment defined by a dynamic, scalable data center fabric, a workload really can run anywhere; the resources needed to support a workload can come even from an outside service provider in a cloud-computing model.

Cisco Cloud Data Center Technology Architecture

Figure 3. Cisco Cloud Data Center Technology Architecture



The technology architecture in Figure 3 represents a next-generation cloud data center. It is based on Cisco's and the ecosystems partners' data center building blocks. The above technology architecture represents only a sample of building blocks of a cloud data center. Moreover, the end-state technical architecture would not only contain the components listed above and below but would also be governed by different types of service and regulation/compliance requirements.

Other key software components are

- Business applications for service orchestration
- Service delivery management applications for service discovery, mapping, and Compliance
- SLA metering, measurement, and billing application for accountability
- Web and business logic hosting applications such as databases, and application and web servers

Other key facilities components are

- Power and cooling components
- Data center physical construction components
- Racking and cabling components

Cisco partners with software application and data center facilities solution providers in the above segments to provide a comprehensive cloud data center solution.

Trust in Cloud Data Center

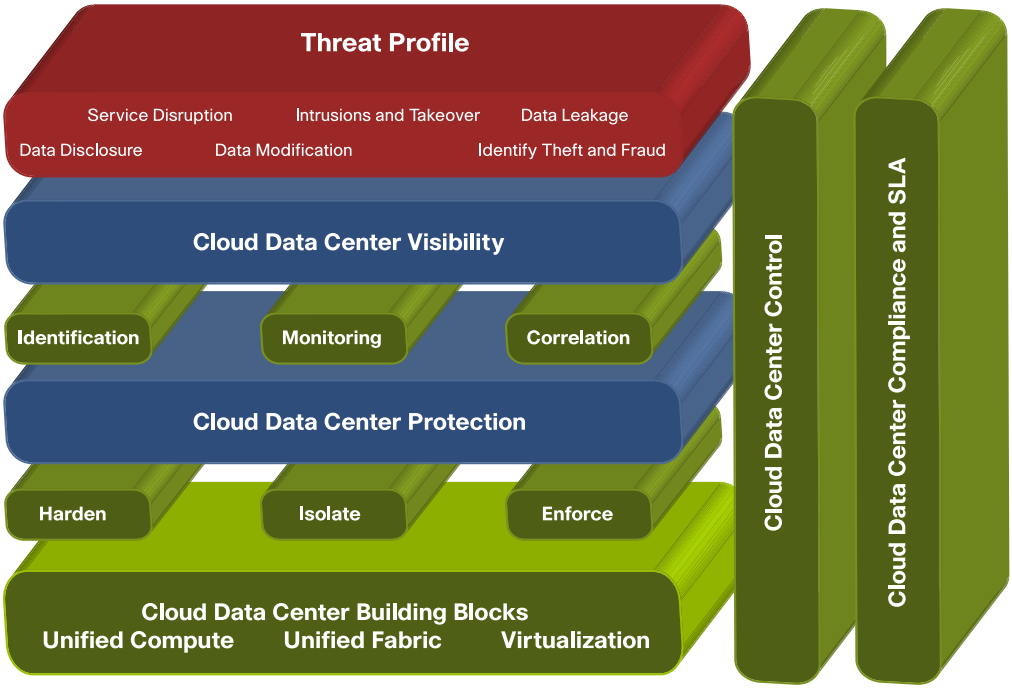
Cisco also brings the following security- and trust-related considerations in the infrastructure models of cloud computing. Cisco believes that gaining the advantages of cloud computing in the enterprise begins with establishing a trusted approach to the cloud. Just as we trust a financial institution with our valuables and monetary assets, a similar level and attributes of trust need to be established in cloud architecture. Hence the definition of private and virtual private clouds is based on the trust domain in addition to physical presence domains. The network can uniquely address trust in private clouds.

Trust in a cloud data center centers on several core concepts:

- Security: Traditional issues around data and resource access control, encryption, and incident detection are factors here.
- Control: The ability of the enterprise to directly manage how and where data and applications are deployed and used.
- Compliance and service-level management (SLA): This concept refers to contracting and enforcement of service-level agreements between varieties of parties, and conformance with regulatory, legal, and general industry requirements.

Cisco adopted the above core concepts in their solutions and services for cloud computing.

Figure 4. Cisco Secure Cloud Data Center Framework



Cisco has developed the Secure Cloud Data Center Framework depicted in Figure 4. This framework portrays the threat model of a cloud data center and the measures that one can take to mitigate security risks. Additionally, the framework shows the overarching controls, compliance, and SLA components. The key take-away in cloud data center security is that security should not be an afterthought or a building block; it should be pervasively implemented across all layers of architecture.

The threat profile consists of elements such as service disruption, intrusion takeover, data leakage, data disclosure, data modification, and finally, identity theft and fraud. A cloud data center would be implemented with visibility and protection aspects across all building blocks.

The elements of cloud visibility are enumerated as shown in Table 1.

Table 1. Cloud Visibility

Identification	Monitoring	Correlation
Firewall Deep Packet Inspection Digital Certificates	Intrusion Detection Anomaly Detection Network Management Network Flow Data Collection Packet Capture Endpoint Monitoring Event Monitoring	Event Analysis and Correlation

The elements of cloud protection are enumerated as shown in Table 2.

Table 2. Cloud Protection

Harden	Isolate	Enforce
Baseline Security Endpoint Security Link and System Redundancy	VLANs Virtual Machines Firewall Access Control Policies SSL Offloading Trust Sec Framework	Stateful Firewall Access Control Intrusion Prevention Endpoint Security Content Filtering L2 Protection (CISF)

Control

There are several dimensions to the control aspect of cloud data center security architecture. These dimensions range from control provisions for the data to the access management systems. As an initial step, the cloud data center should review the security baseline of the most stringent requirements. Typically data centralizationcan lead to greater insider threat; hence a compartmentalization strategy is a key component of data control. Moreover, unencrypted data in a cloud data center should be considered as part of risk management and control policy. Therefore private and public clouds should review their data encryption policies and their adherence with SLA and contract compliance.

As discussed earlier, virtualized computing is a foundational component for cloud data centers. Hence operating systems (in an virtualized settings) should be instruments with appropriate security profiles to provide layered security controls. Also, it would be prudent for cloud data center consumers to consider providing trusted virtual machine images, which already conform to the consumer's internal security policies. Additionally, important aspects of control include administrative access and control of virtualized operating systems, with strong authentication, integrated with identity management, and tamper-proof logging and integrity-monitoring tools. Identity and access management is a critical component of cloud data center security architecture. Public and private cloud data centers would need to implement robust federated and standards-based identity management architectures and strategy. Finally, cloud-based application architectures should also consider single sign-on (SSO) for private cloud applications and leveraging this architecture for public cloud applications.

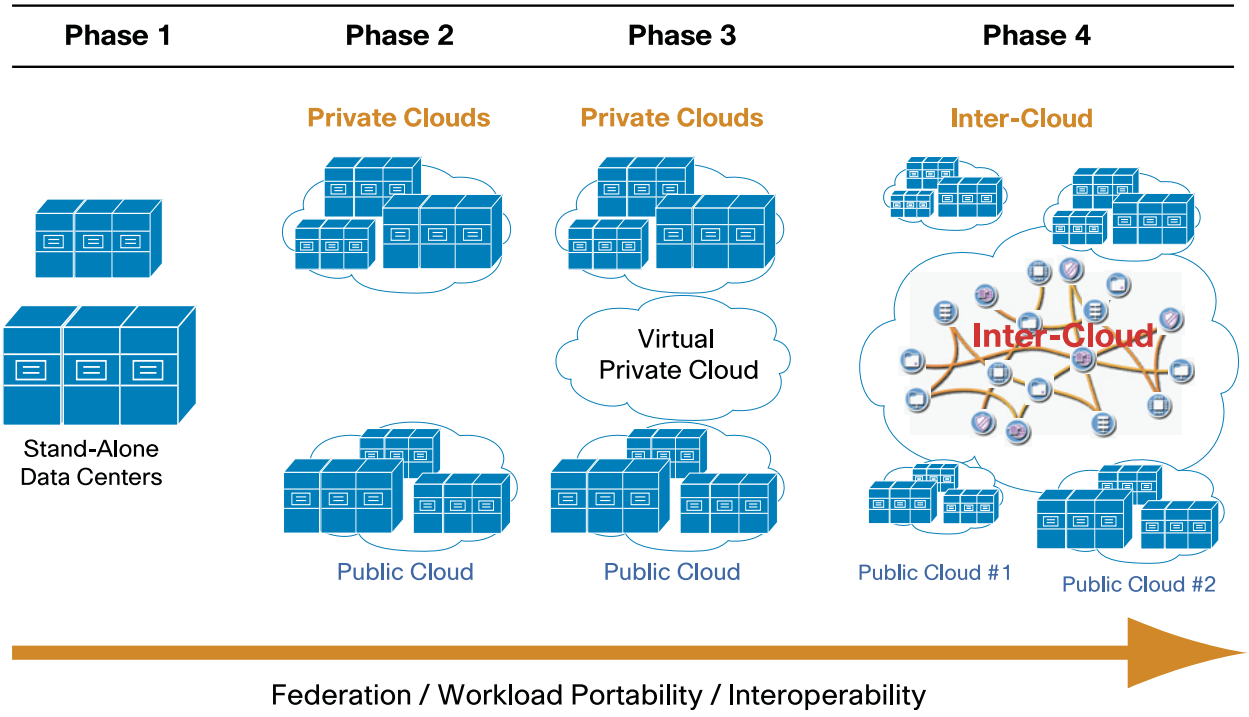
Compliance and SLA

The compliance and SLA aspects of cloud data center security architecture are multifaceted. First, public managers and government executives need to understand the different components of a cloud data center that need to be compliant. These components may include physical data center facilities, infrastructure systems, and data itself. In the case of data and systems compliance, not only do classification requirements need to be addressed, but also the location (both source and copies of source) needs to be considered. Auditing and assessments requirements (both for risk and privacy), as mandated by the regulation, also need to be addressed. SLA contracts (internal or external) for cloud services are key compliance enforcement mechanisms and should be synchronized with an organization's

unique requirements. In a cloud data center, SLA contracts should be treated as a mechanism to map SLAs to architecture and service delivery. Some examples of SLA contracts-driven compliance in a cloud data center architecture could include understanding the secondary uses of consumer data and related systems, the prohibition of this use, if necessary, and the identification of the potential for cross-classification of data transfers, and its prohibition, if necessary. The above considerations lead to increased security, performance, and availability metrics for the consumers and an increased quality of the overall cloud data center security architecture.

Phased Evolution of Cloud

Figure 5. Phased Evolution of Cloud



Cisco envisions a phased infrastructure build–out of cloud in the industry, Figure 5. An enterprise path to private cloud will almost always begin very simply with a pilot deployment, typically targeted at mission support, and highly variable workloads, such as development, testing, training, and demonstration labs, in which it is highly advantageous for end users to self-provision systems and/or storage. Pilot deployments may include traditional grid and batch computing applications, which typically involve intensive data processing for the length of a single request or job, at which time resources can be freed for the next application. Other deployments could include intranet applications that have widely varying loads, such as accounting systems and expense reporting and benefits systems. These pilots are typically very visible internally, and are run in conjunction with new or existing server and storage virtualization initiatives.

Once governments get comfortable with the reliability and economic advantages of their private cloud pilot systems, they can move to the next steps of scaling the infrastructure for newer sets of infrastructure and application. Resource pools can be expanded to include more of existing, as well as newer, storage, server, and networking infrastructure. This could be implemented application-by-application or a data center at a time. Private clouds will also expose opportunities for new applications, research methods, or business processes that were not possible in the past. As a result, new application architectures would become inexpensive to deploy and maintain.

Once the enterprise has multiple private clouds leveraging disparate infrastructure and applications, likely in a variety of different data centers, it would becomes advantageous to allow each cloud to federate unused resources with the

others, and request additional resources should it reach full capacity. Federation should not be thought of as building a single private cloud from a variety of data centers, but rather allowing a private cloud instance to borrow from others as required. The other private clouds would continue to operate their own infrastructure management systems that would simply cooperate with the requestor system in the case of federation. This arrangement gives each private cloud the illusion of having significantly more resources available than it actually manages itself. Federation also allows for interesting approaches towards disaster recovery and global distribution of services (for disaster avoidance, for instance).

The federation aspect would introduce a new set business and procurement models, where technology will allow service providers to offer unique services to private cloud users. These services, known as virtual private clouds, will allow customers to consume service provider infrastructure clouds as part of their private clouds. In other words, the customer can extend the trust boundaries to include virtual private cloud infrastructure. Finally, once standards are introduced for private cloud/virtual private cloud federation, it will be possible for enterprises to choose from a variety of cloud vendors dynamically, where vendors and partners will leverage each other's infrastructure. Such a standards-based cloud market is called an inter-cloud, and it will truly change the way that IT resources are acquired and consumed. A standards-based open cloud also forms the basis of the inter-cloud, the public cloud internetwork.

Additional Considerations

Interoperability

One of the future challenges that Cisco sees in the cloud environment is interoperability among the clouds. In a classic cloud use case scenario, enterprises would want to help ensure an exit or a migration strategy across multiple clouds, thereby avoiding the perils of a vendor lock-in. This strategy creates an imperative need for an interoperable set of functions via a standardization process. Cisco is actively working with standard bodies and other partners to help ensure these challenges are addressed as clouds become pervasive.

Enabler Ecosystem

There are many complex domains within a cloud data center infrastructure. Typical examples of these domains are computing, network, storage, security, software applications and service management. Within those domains, there are several areas of complexity, including integration, interoperability, operation, scalability, and compliance. Thus as enterprises start adopting private clouds, they would need a healthy ecosystem of cloud solution providers, which would ease the burden of the above mentioned complexities by providing interoperable, pre-integrated, pretested, pre-validated, and coordinated solutions. Cisco is a part of one such ecosystem of cloud infrastructure providers.

Conclusion

Public sector and federal government agencies can take their first step with Cisco toward cloud computing and private cloud data centers. Customers should start with applicable and manageable use cases as initial points of entry into cloud. They can start with identifying potential opportunities for cloud infrastructure. Customers should also consider and develop ancillary aspects of their IT organization to adopt private cloud architectures. Some of these aspects could be:

- Map cloud architecture to enterprise architecture as part of an IT roadmap
- Create a cloud task force or steering committee as part of current architecture boards to evaluate cloud adoption
- Develop a cost and agility business case to justify further adoption
- Evaluate technical and organization alignment to aid cloud adoption
- Perform an information inventory to assess which data assets can be hosted in external clouds

Finally, in addition to the initial steps, customers should investigate utilizing external virtual private clouds for burst or new applications. As per the Cisco vision, cloud service providers will offer both public and private cloud services in the form of virtual private clouds that will be consumed and controlled within private cloud data centers. Cisco can deliver comprehensive cloud data center architectures, as IT infrastructures evolve and deliver cost-effective, ubiquitous, easily accessible, reliable, and efficient services.

Additional Cisco Information

Table 3. Additional information about the Cisco solutions described in this document can be found at the following websites.

Description	URL
Cisco Solution URL Cisco Cloud Computing Solutions	http://www.cisco.com/go/cloud
Cisco Data Center Solutions	http://www.cisco.com/go/datacenter

About the Author

Kapil Bakshi is the chief solutions architect for Cisco Federal's Data Center Practice. Kapil is responsible for leading and driving data center and cloud computing strategy and initiatives in Cisco Federal. Kapil has extensive experience in strategizing, architecting, managing, and delivering data center solutions to U.S. federal government agencies and enterprise customers. During his career, he has held several architectural, consulting, and managerial positions within the industry. Prior to Cisco, Kapil worked for Sun Microsystems, where he spent a decade working with U.S. federal government and service provider customers. Prior to SUN Microsystems, he worked for Hewlett-Packard and several government system integrators in consulting and product development roles. Kapil is native of Washington DC, and holds both a BS in electrical engineering and a BS in computer science from the University of Maryland, College Park, as well as an MS in computer engineering from Johns Hopkins University and an MBA from the University of Maryland, College Park. He also holds U.S. patents for data center and related solution sets. He can be reached at kabakshi@cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-555787-00 08/09