Cisco's Cloud Adoption Strategy for Public-Sector Organizations

Introduction

Federal, state, and local government agencies are adopting private and community clouds to reduce costs and increase agility. Carefully selecting the architecture and planning the transition will help increase benefits and avoid risk.

This paper is intended for government business managers and IT professionals who have already decided in principle to adopt cloud computing and are now planning the transition. This paper is a follow on to the Cloud Powered by the Network: What Business Leaders Must Know, paper, published by Cisco.

This paper explains:

- Factors to consider when creating the business case for private clouds
- Process to private cloud rollout
- Ready-to-use architectural building blocks that avoid the time and costs of integrating computing, networking, storage, and virtualization
- Examples of public cloud services useful for government organizations

We would also like to draw attention to a point that is often overlooked: **the network is essential for delivering cloud services**. One of the fundamental characteristics of cloud is that the services are delivered in a location-independent fashion, making the network an essential platform for delivering cloud.

The role of the Network Platform can be enumerated in the following fashion:

Seamless access to critical data, services, resources, and people

- Core fabric connects resources within the data center and data centers to each other
- Pervasive connectivity links users and devices to resources and each other

National Institute of Standards and Technology Cloud Computing Definition

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with little management effort or service provider interaction.

- Essential characteristics of clouds include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measurement of the services that each subscriber consumes.
- Service models include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).
- Deployment models include private clouds used for a single organization, community clouds shared by multiple organizations with shared concerns, and public clouds. Hybrid clouds combine two or more clouds that can share resources when appropriate.

- Identity and context based access to data, services, resources, and people

Granular control of risk, performance, and cost

- Manages and enforces policies to ensure security, control, reliability, and compliance
- Manages and enforces service level agreements and consistent quality of service within and between clouds, enabling hybrid models and workload portability
- Meters resources and utilization to drive transparency around cost and performance

Robustness and resilience

- Supports self-healing, automatic redirection of workload, and seamless rollover
- Scalability enables on-demand, elastic power through dynamic configuration

Innovation in Cloud-specific services

- Context-aware services appreciate identity, location, proximity, presence, and device
- Resource-aware services discover, allocate, and pre-positions services or resources
- Comprehensive insight accesses and reports on all data that flows in the Cloud

To execute on our strategy to enable to realize the benefits of cloud, Cisco has built an innovative portfolio with open enabling ecosystem and standards that provides choice and flexibility to governments. From architectures that detail how to design clouds, to the actual IT infrastructure needed to build and connect clouds, to services and solutions that can be consumed using any of the cloud deployment models in conjunction with service providers. As a result, here are some of the salient benefits of cloud deployment model, in a public sector domain:

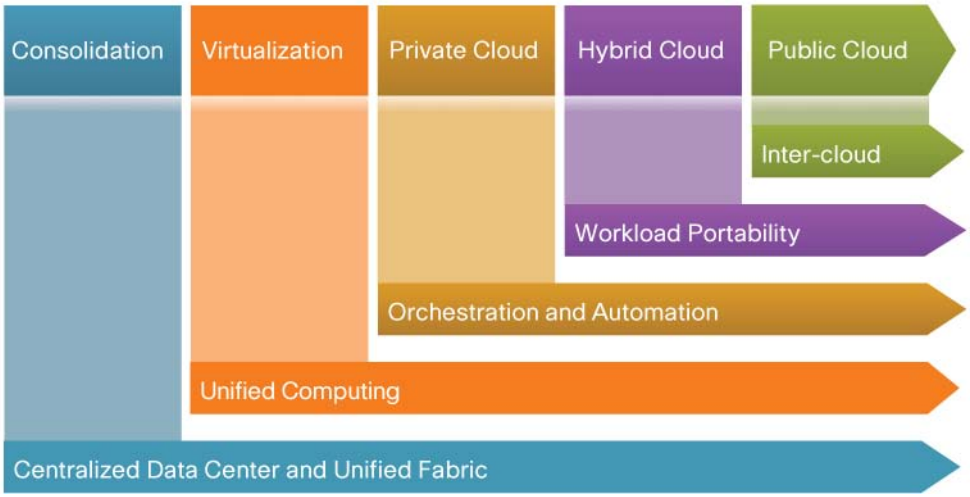
- **Lower costs**: Capital expense decreases for departments that use private cloud services because they can add resources in small increments, paying only for what they need.
- **Business flexibility**: Agencies can quickly provision new IT infrastructure for projects that support the mission, often in minutes, compared to weeks with traditional architectures. Cloud computing also shortens the procurement and acquisition processes.
- **Increased efficiency through automation**: Departments can add or decrease resources dynamically. Automation offloads government IT groups, freeing resources to focus on the mission.
- **Environmental sustainability**: Cloud computing consolidates multiple servers, switches, and cables into a single energy-efficient platform that uses less power and cooling.

Cloud computing architectures vary, and the best one for a given agency depends on mission needs, including security requirements. Therefore, to increase business value and reduce risk, agency IT teams need to carefully consider the business case for their agency and map it to the characteristics of several pretested cloud architectures, described later in this document. In general, to confidently adopt cloud computing, government organizations need confidence that the cloud model supports trust, security, and standardization.

Why Private Cloud?

As part of its vision for cloud evolution, Cisco has developed a roadmap for the evolution of cloud architectures (Figure 1). This roadmap progresses through the main phases of cloud infrastructure evolution and architectural enablers that Cisco brings to government and to cloud computing. The initial phases are based on the constructs of pervasive virtualization, and the final phases show adoption of cloud computing.

Figure 1. Cisco Cloud Evolution Roadmap



A private cloud is built specifically to provide cloud services internally to an organization. Private clouds can be in a co-located facility or in an existing data center. A private cloud gives a high level of control over the cloud services and the cloud infrastructure to an organization.

Note that, in Cisco's vision, private cloud is the first form of cloud computing that governments and enterprises will adopt as they move to cloud computing. The adoption of community clouds will be in parallel with the adoption of private clouds and will be followed by adoption of hybrid and consequently public cloud in the government sector.

The traditional benefits of cloud computing will be experienced initially through the adoption of private and community clouds internally or by a group of public-sector institutions. Hence, the benefits of cost efficiencies, agility to adapt to mission demands, improved automation, focus on core competency, and sustainability will be achieved in private clouds first. As hybrid and public clouds mature for adoption by governments, these benefits will be achieved in parallel with hybrid and public clouds.

Also, the public sector can leverage existing underutilized assets that have been paid for and develop private or community clouds for their usage. Thus providing less motivation to move to public clouds as long as those assets can be used without significant changes. In addition to the short-term benefits achieved by deploying an internal private cloud, the process of deploying an internal cloud helps ensure cloud readiness.

Considering the public sector's unique concerns and consideration, private cloud stands out an initial step in the journey to cloud computing. Table 1 lists public-sector concerns and maps them to a cloud delivery model.

Table 1. Public Sector Concerns and Private Clouds

Public-Sector Concerns	Public Cloud	Community Cloud	Private Cloud
Ease of acquisition	X	X	X
Trust and security		X	X
Ease of operational insertion			X
Little effect on culture			X
Ease of portability		X	X
Standards and common specification			X

Additionally, public-sector information assurance policies result in unique requirements that few public cloud providers can currently meet. Hence, private clouds can offer the benefits of public clouds with additional integrated security capabilities not available in public clouds.

Creating a Business Case for Cloud Computing

At the onset of the journey to cloud computing, a critical step to consider is creation of a business case demonstrating how private cloud can help meet the government agency's mission more efficiently and effectively. As government institutions consider moving certain applications (and related infrastructures) to the private cloud while retaining others on traditional infrastructure, they need to adopt a cloud-readiness approach and consider several important factors. Here are few factors that determine the readiness of applications (and related infrastructures) for migration to a cloud and eventually contribute to a business case for private cloud:

- **Strategic factors**: These entail review of the strategic value of data, applications, and related infrastructure and their mapping and effects on migration to a private cloud. Additional topics to consider are mandates, regulations, policies, and procurement models. This factor is also highly dependent on the nature of the mission and strategic objectives of the specific agency or public-sector institution.
- **Business and mission process factors**: These entail an assessment of how private cloud adoption of technology-enabled business processes will transform business and mission processes. Mappings of applications to the mission and business processes are reviewed, and the maturity of applications and related data center infrastructure to transform and provide the services through an internal private cloud is assessed.
- **Economic factors**: These entail review of savings, investments, and metrics to develop an economic model to justify adoption of private cloud.
- **Risk factors**: While evaluating cloud computing, organizations need to adopt a risk-based approach. This is a crucial part of building a business case and will be evaluated in detail in later sections.

These factors all are important to consider; however, depending on the nature of the cloud project and organization, these factors may not have equal priority and may have weighted considerations. The following section provides further details about business process and economic factors and provides a framework for evaluating the movement toward cloud computing.

Different agencies will weight these criteria differently. For some, the greatest consideration may be cost savings or business process transformation; for others, helping ensure compliance with privacy regulations may be paramount. The following section provides further details about business processes, economic and risk criteria and provides a framework for evaluating the decision factors for private cloud.

Business and Mission Process Factors

As part of the business and mission process analysis, one needs to review the application environment and the related data center infrastructure environment for readiness and for candidates for transformation to a private cloud. This analysis will contribute to the overall business case for private cloud.

In analyzing the application environment, review the following to help determine readiness and affinity for a private cloud:

- Application profiles and attributes
- Application mapping to mission and business processes
- Application use analysis
- Application heat map based on importance and significance to the mission
- Application dependency model, assessing dependency on other data sets, processes, and people

- Migration of the application to a multitenant virtualized environment.
- Application scalability for a variable workload
- Application attributes for dynamic and agile provisioning
- Application adherence to standards and common specifications
- Application performance metrics and instrumentation for mapping to service-level agreements (SLAs)
- Application availability architecture in a multitenant virtualized environment

In assessing the readiness of the data center for cloud computing, review such factors as the following:

- Refresh lifecycle of equipment
- Scalability and capacity for greenfield and brownfield deployments
- Availability design to meet contracted SLAs
- Operational maturity within governance frameworks such as ITIL and ITSM
- Architecture to enable adoption of new virtualization and multitenancy technologies
- Security and compliance architecture relevant to private cloud
- Workload mobility and rapid provisioning
- Adherence to standards and common specifications

After reviewing application and related data center environments, one should begin to see which applications are ready and capable candidates for movement to a private cloud model and would contribute to the overall cloud business case.

Economic Factors

As part of business case for a private cloud, one needs to gather, calculate, benchmark, and analyze certain foundational metrics. As a start, you need to benchmark and develop a baseline enumeration of these metrics that can be used for savings comparisons as your organization adopts a private cloud deployment model. These metrics assess financial, productivity, and technical details, which directly and indirectly map to the economic factors. Note that the economic factors not only assess financial cost efficiency, but also agility and productivity gains. Table 2 presents a sample of these metrics.

Table 2. Metrics for evaluating Private/Community Cloud business case

Financial Metrics	Productivity Metrics	Infrastructure Metrics
• Total cost of ownership (TCO) • Net present value (NPV) • Return on investment (ROI) • Return on asset (ROA) • Discount payback period (DPP) • Cost per virtual machine	• Hours required to procure end-to-end system • Hours required to provision end-to-end application • Consolidation ratio (virtual:physical) • Number of IT administrators per physical and virtual asset	• Consolidation ratio (physical:virtual) • Asset utilization • Application response time • Power use effectiveness (PUE) • Kilowatts per virtual machine

Community Clouds for State and Local Governments

Community clouds, shared by multiple departments or municipalities, provide a framework for reducing capital expenditures and operating expenses while enabling information sharing. Examples include programs to share operational data, provide consistent information to citizens, and jointly manage initiatives such as transportation, parks and recreation, property taxation and revenue, criminal justice, and police operations.

The benefits of community clouds are so overwhelming that most CIOs forego formal ROI studies. Multiple studies reveal the following results:

- Consolidating email and video-based collaboration services typically saves 24 to 65 percent.
- Offering customer relationship management and human resources applications as SaaS reduces costs by up to 26 percent, with a 12- to 24-month payback.
- Offering IaaS, PaaS and SaaS typically reduces provisioning time from 40 to 70 hours to less than 30 minutes, increasing agility.
- Launching an application with a PaaS cloud takes less than a week, compared to 5 to 7 weeks with traditional IT infrastructure.
- Virtualizing computing and storage assets saves 35 percent on average without automated provisioning, and 52 percent with automation.
- State and local government agencies can quickly implement community clouds using the Vblock and SMT architecture from Cisco, VMware, EMC and Netapp.

Sources: Forrester Research (July and August 2009), Information Week (June, 2010), IT Business Edge Study (2008), "Service Management in Action" study by IBM Tivoli (2009), and IDC (July 2008)

The financial analysis consists of comparing the private cloud architecture to traditional IT models. It includes both initial capital costs and ongoing operational costs, as listed here:

- **Hardware costs**: Servers, storage, network equipment, racks, cables, etc.
- **Software costs**: Basic data center software for the OS and virtualization, backup software, security software, etc. and business application software licenses
- **Implementation and migration costs**: Labor and tools for engineering and planning support during the transition phase and for hardware and software maintenance
- **Facilities costs:** Power, cooling, and space for the cloud data center
- **Operational and maintenance costs**: Ongoing support of the cloud infrastructure, including hardware and software maintenance and associated labor

As you develop a business case for private cloud, you can review the savings and investments. Table 3 provides an initial snapshot of a traditional data center cost model, with relevant investment and initial review of savings and ROI on traditional and new investments.

Table 3. Private Cloud Investments and Associated Savings

Traditional Cost Model and New Investments	Savings and ROI from Adoption of Private Cloud
• Traditional capital expenses (hardware, software, and facilities) • Traditional operating expenses (operations and support and skills training) • New virtualization software • New cloud automation and orchestration software • New greenfield or brownfield data center facilities	• Consolidation of assets • Increased utilization • Reduced energy and depreciation costs • End-to-end (rather than siloed) optimization • Reduced time and effort in provisioning and procurement • Improved agility and efficiency of operations and support functions • Improved productivity of end users such as developers, testers, and mission and business constituents

Risk Mitigation and Trust Factors

In evaluating cloud options, one needs to adopt a risk-based approach. A sound mission process and economic evaluation will be less advantageous if it poses too much risk. To evaluate and mitigate risks posed by private cloud adoption, the Cloud Security Alliance has developed a set of processes and considerations.

Follow these basic steps when considering data and application assets in a typical enterprise:

Federal Risk and Authorization Program

The Federal Risk and Authorization Program (FedRAMP) is a risk management program for large outsourced and multiple-agency information systems. Created to support the U.S. government's cloud computing plan, FedRAMP authorizes and continuously monitors IT services that are used by multiple federal departments and agencies, avoiding duplication of effort when multiple agencies evaluate the same cloud service provider. Although FedRAMP verifies the services, agencies are encouraged to evaluate services further based on their own use cases and privacy and security requirements.

FedRAMP bases its evaluations on a unified risk management process that includes security requirements. The plan is to eventually expand FedRAMP beyond cloud services.

Step 1. Evaluate the asset. Determine which data and application assets can be considered for cloud adoption. To do this, you need to evaluate the confidentiality, integrity, and availability dependencies of data and application assets.

Step 2. Map assets to cloud models. Map the data and application assets you evaluated in Step 1 to the cloud deployment model: private, public, or community cloud. You may choose to adopt a private cloud model initially, so you can learn from an internal instance, before you evaluate an external cloud provider.

Step 3. Determine the potential data flow. Map the data flow between organizations, the private cloud, and other user nodes. The goal of this exercise is to identify data leakage and risk exposure points.

Step 4. Develop a trust strategy that addresses operational issues and governance. A comprehensive trust strategy addresses security, control, compliance, and SLA adherence.

These steps provide a framework for understanding risk tolerance, cloud deployment options, and exposure points for sensitive information.

Public-sector organizations should also review the governance and operational considerations listed in Tables 4 and 5 as part of developing a trust strategy.

Table 4. Governance Considerations for Trust Strategy

Areas of Consideration	Details
Enterprise risk management	• Legal precedence for agreement breach • Ability to assess cloud deployment model • Responsibility to protect sensitive data
Legal and electronic discovery	• Protection requirements for information systems • Security breach disclosure laws • Regulatory, privacy, and international laws
Compliance and audit	• Maintaining and proving compliance in a cloud model • Cloud effects on internal security, regulatory, and legislative factors
Information lifecycle management	• Identification and control of data • Data confidentiality, integrity, and availability • Compensating data controls
Portability and interoperability	• Movement of data and services from one cloud to another • Interoperability between clouds

Table 5. Operational Considerations for Trust Strategy

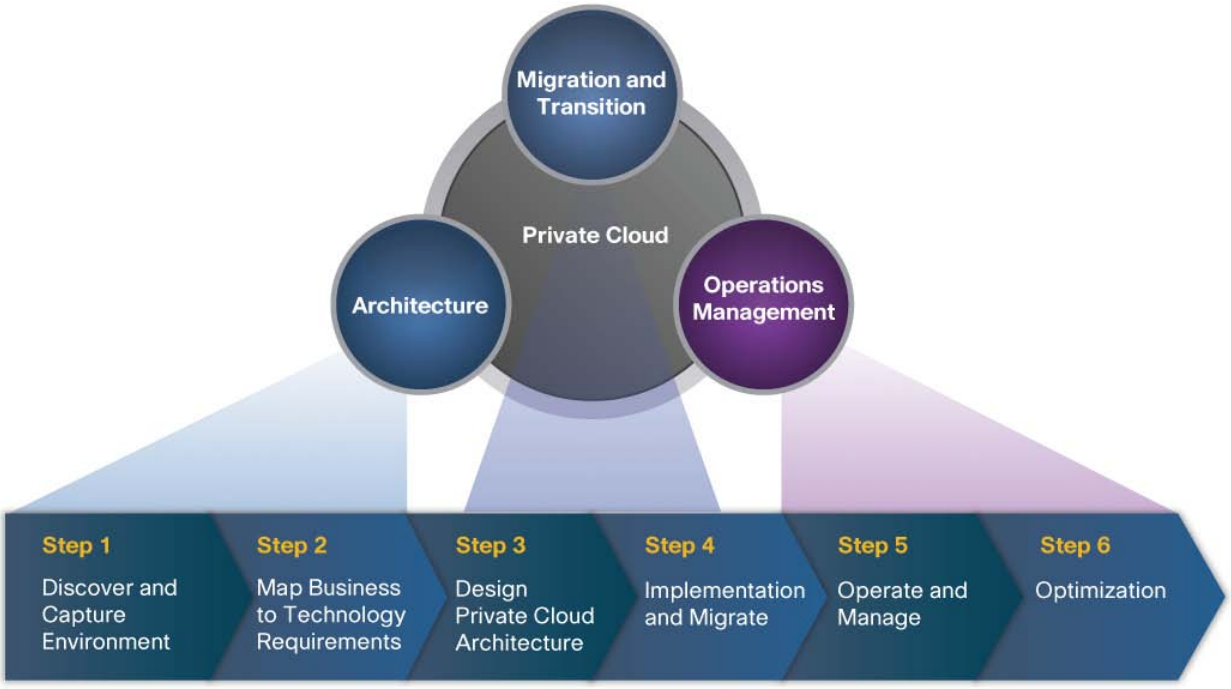
Areas of Consideration	Details
Business continuity and disaster recovery	• Traditional security with continuity and continuation of operations (COOP) requirements • Enterprise risk management (ERM) and COOP models
Data center operations	• Evaluation of data center architecture and operation • Stability of services for current and target data center
Incident response, notification, and remediation	• Adequate incident handling and forensics • Evaluation of complexities of current incident program
Application security	• Evaluation of migration to cloud with proper security • Evaluation of design of application for cloud deployment
Encryption and key management	• Identification of proper encryption management • Protection of access to resources and data
Identity and access management	• Challenges related to extending identity into the cloud • Readiness to conduct cloud-based identity and access management
Virtualization	• Risk with multitenancy • Virtual machine isolation and hypervisor vulnerabilities

Thus, a holistic trust strategy includes security, control, compliance, and SLA adherence. You can use the considerations listed in Tables 4 and 5 to identify risk exposure and produce a list of applications and infrastructure that are suitable for moving to the private cloud first.

Cloud Rollout Process

Cisco recommends a six-step process to roll out a private cloud in government organizations (Figure 2). The steps can be grouped into three phases: architecture development, migration and transition, and operation and optimization. Following this process reduces risk and helps ensure that the agency derives the most mission benefits from the cloud.

Figure 2. Cisco Process for Private Cloud Adoption in Government



Step 1. **Discover and capture environment.** Create an accurate inventory of the application and data center assets related to the evaluated business process. This inventory should includes application and data center attributes, current state, and prioritized mappings to the mission process.

Step 2. **Map business to technology requirements.** This step typically includes analysis of the business case, SLAs, enterprise standards, governance requirement artifacts, organizational structure, and IT operations attributes. This step also includes cloud service use case development through application dependency mapping and application rationalization.

Step 3. **Design private cloud architecture.** Envision the target architecture of the cloud service and develop a detailed action plan including:

- Platform architecture design (computing, networking, storage, virtualization, and facilities) and systems management tools
- Application implementation and migration plan with migration group analysis
- End-to-end security plan, including identity and trust, event monitoring, policy enforcement, isolation, and resiliency
- Cloud operation and SLA delivery readiness plan
- Chargeback plan for users and departments

The next section of this document describes four private cloud architectures suitable for government and other public-sector institutions.

Step 4. **Implementation and migrate.** This step applies to new data centers (greenfield) as well as redesigned data centers. Begin by staging and validating the private cloud platform to prepare for production. Next, migrate existing applications to the cloud platform or provision new applications. The best migration approach can vary based on the mission and operational constraints. Some critical implementation and migration strategies will depend on the mission and operation constraints. Hence, strategies of lift and shift or parallel operations and cutover or physical-to-virtual migration could be adopted. Then applications could be grouped into dependent migration groups and migrated in a coordinated fashion. Treat this step as an opportunity to rationalize applications based on the agency's current mission requirements and technology. This step becomes even more important as you contemplate a large-scale private cloud deployment.

Step 5. **Operate and manage.** Perform standard operation and management functions: monitoring, administration, provisioning, change management, and SLA management.

Step 6. **Optimization.** An ongoing process, optimization involves continual analysis of cloud performance, availability, and SLAs.

Cisco recommends that agencies operating private clouds establish a program management office (PMO) and an architecture management office (AMO). The mission of the PMO is to provide project governance, communications planning, risk mitigation, and ongoing management status updates for on-time, coordinated delivery of the target architecture. The AMO aligns the technology and operations architectures with requirements and applies standardization and automation to reduce costs, complexity, and risk. Both offices provide crucial input to the six steps.

Programs to Accelerate Government Cloud Adoption

The Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) was formed to accelerate the development of cloud standards and increase the level of confidence in adopting cloud computing until standards are formalized. SAJACC provides a web portal, hosted by NIST, providing information about interim specifications and the extent to which they support main cloud computing requirements. The portal includes:

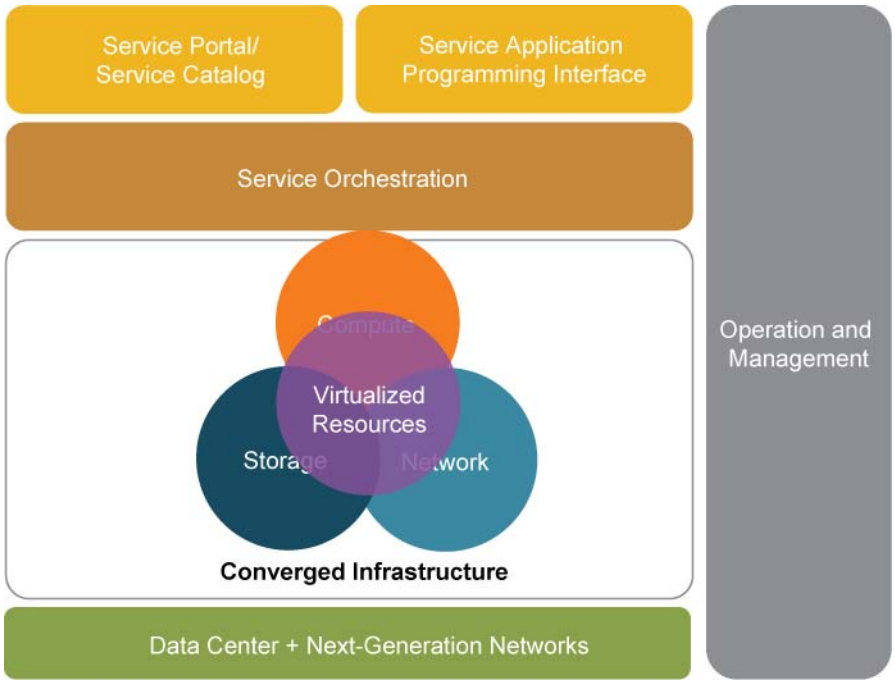
- Cloud computing use cases verified by cloud computing stakeholders in academia, government, and industry; the use cases demonstrate portability, interoperability, and security
- Documented cloud system interfaces and reference implementations for validation against the use cases
- Test results showing the extent to which different interfaces can support individual use cases

SAJACC will continue to identify new interfaces and their corresponding reference implementations. SAJACC welcomes input from all stakeholders with an interest in cloud computing standards.

Private and Community Cloud Technologies, Architectures, and Building Blocks

As mentioned previously, several factors (strategic, business process, economic, and risk) shape the case for the adoption of private cloud. However, these factors cannot be used to formulate the use case for transition to the cloud model without appropriate technologies, designs, and building blocks. Technology acts as a catalyst for making the use case a reality. Cisco has a comprehensive portfolio of solutions to help public-sector institutions with their cloud architectures. Figure 3 provides a functional view of Cisco's private cloud architecture and architectural roadmap for achieving a private cloud model.

Figure 3. Cloud Reference Architecture



The Cisco® technology portfolio that enables the cloud architectures and building blocks includes the following products:

- **Cisco Unified Computing System®:** Cisco UCS B-Series Blade Servers and UCS C-Series Rack-Mount Servers
- **Unified fabric:** Cisco Nexus® Family
- **SAN products:** Cisco MDS 9000 Family
- **Virtual switching:** Cisco Nexus 1000V Switch and virtual interface cards
- **Core switching:** Cisco Catalyst® Family
- **Routing:** Cisco 7600 Series Routers and CRS-1 Carrier Routing System
- **Security:** Cisco ASA Adaptive Security Appliances and firewall, intrusion detection system (IDS), and intrusion prevention system (IPS)

A private or community cloud infrastructure has many complex domains. Typical examples of these domains are computing, network, storage, security, software applications, and service management, and areas of complexity include integration, interoperability, operation, scalability, and compliance. Thus, as enterprises start adopting private clouds, they need a healthy ecosystem of cloud solution providers to ease the burden of these complexities by providing interoperable, preintegrated, pretested, prevalidated, and coordinated solutions. Cisco is a part of an ecosystem of such cloud infrastructure providers.

Self-Service Provisioning: Cisco IT Elastic Infrastructure Services

The Cisco IT team wanted to build an internal private cloud for IaaS that internal customers could use to self-provision servers, storage, and network resources. Top goals included low TCO, rapid provisioning, and high service resiliency and availability. Operating expenses account for more 50 percent of TCO for virtual machines, so Cisco IT wanted to automate manual processes associated with provisioning, including procurement, installation, configuration, and securing of resources.

The result is Cisco IT Elastic Infrastructure Services (CITEIS). A framework for providing IaaS, CITEIS combines virtualization and automated service management. Cisco departments and project teams access a web-based service catalog to self-provision servers, storage, and network resources from a shared pool, hosted using the Cisco Unified Computing System and the Cisco SAN. "Elastic" means Cisco users can expand or contract resources on demand. Cisco IT does not spend any time on provisioning tasks, but simply bills internal users based on usage. Benefits of CITEIS to date include:

- 32 percent lower TCO compared to IaaS based on virtualization alone
- Increased agility (Before Cisco automated IaaS provisioning, Cisco users received new infrastructure in 2 to 3 weeks, requiring 17 hours of IT staff time. In the CITEIS environment, with automation, users can begin using infrastructure in 15 minutes, with no IT staff time.)
- Higher service quality through elimination of human configuration errors
- Resiliency, enabled by virtualization
- Environmental sustainability, measured by the number of virtual machines per kilowatt consumed

Cloud platforms consist of integrated computing, networking, storage, and virtualization software, and sometimes other software. Cisco has developed a collection of architectures and building blocks based on its technology portfolios in conjunction with ecosystem partners such as EMC, NetApp, VMware, and BMC. Rather than incurring the time and costs of internally designing, integrating, and testing a cloud platform, government IT groups can use one of several preintegrated, pretested cloud building blocks from Cisco and its ecosystem partners:

- Vblock Infrastructure Packages from the Virtual Computing Environment (VCE) coalition
- Secure Multitenant (SMT) architecture
- Virtualized Multitenant Data Center (VMDC)
- Cisco Containerized Data Center (CCDC)

Vblock Architecture

Jointly designed by the VCE coalition, a collaboration of Cisco, EMC, and VMware, Vblock™ Infrastructure Packages are pre-engineered, tested, and validated units of IT infrastructure that include computing, networking, storage, and virtualization resources (Figure 4). They deliver predictable performance, availability, and capacity. Each Vblock Infrastructure Package contains:

- VMware vSphere and vCenter in the Cisco Unified Computing System
- EMC CLARiiON CX4 Series or Symmetrix V-Max Series storage
- Cisco MDS 9000 Family modular Fibre Channel switches

The main benefits of the Vblock infrastructure for private clouds in government include rapid deployment, ease of expansion without disruption of ongoing services, and predictable performance, which enables IT to offer SLAs to departments using the cloud service. Security features include multitenant administration, role-based security, and strong user authentication.

Secure Multitenant Architecture

The SMT building block meets the requirements of government agencies with strong needs for data confidentiality and isolation. This pre-engineered, tested, and validated unit of computing, networking, storage, and virtualization resources consists of the Cisco Unified Computing System, VMware software, and NetApp storage. SMT protects confidentiality throughout the cloud environment using the following security technologies:

- **NetApp virtual storage containers:** NetApp MultiStore technology partitions a single storage system into multiple isolated logical partitions. Authorized users can access only the information in their own virtual storage containers.
- **Cisco Nexus virtual device contexts:** Each Cisco Nexus 7000 Series Switch can operate as up to four virtual switches, or virtual device contexts (VDCs). Each VDC has its own configuration, set of physical ports, and services, keeping each tenant's information separate as it travels across the core network.

- **Cisco VN-Link technology:** Cisco Nexus 1000V virtual switches, closely integrated with VMware vSphere, use VN-Link technology to provide security services to each individual virtual machine. Network and security policies follow a virtual machine as it moves within the Cisco Unified Computing System environment.

Virtualized Multitenant Data Center

The VMDC architecture builds on the Vblock and SMT architectures, adding orchestration for automation and configuration management. This pre-engineered, tested, and validated unit of computing, networking, storage, and virtualization resources consists of a basic IT infrastructure module called the point of delivery (PoD). Both large and compact PoDs are defined, each available with Gigabit Ethernet or 10 Gigabit connectivity.

Orchestration software from BMC enables cloud service to self-provisioned resources. After selecting cloud service options, host applications, and the service level (bronze, silver, or gold), the VMDC system automatically configures all devices, including the Cisco Unified Computing System, storage, and switches. Service orchestration significantly reduces the operational expenses of government cloud services and also accelerates provisioning, potentially from months to minutes. The VMDC architecture incorporates security at each layer of the data center, including the WAN edge, core, aggregation, access, virtual access, computing, and storage layers.

NASA Provisions Cloud Resources to Scientists from Cisco Containerized Data Center

The Nebula program provides cloud-based computing services to NASA scientists and engineers. The main goal of the program is to lower costs by centralizing hardware, using open source software, and offering usage-based billing. NASA decided to build a private cloud instead of subscribing to a public cloud service because its huge data sets require very high network bandwidth, and the agency needs to comply with the Federal Information Security Management Act (FISMA). Nebula resides in a 40-foot container at the NASA Ames Research Center in Mountain View, California, which contains a Cisco Unified Computing System, Cisco network devices, and rack-mount servers. Nebula automatically adjusts the computing and storage resources available to web applications as demand fluctuates.

Cisco Containerized Data Center

Agencies that need data center space for the cloud platform can quickly set up a Cisco Containerized Data Center (CDC). An ISO-designed container (40 feet long, 8 feet wide, and 9.6 feet high), the Cisco CDC has a smaller footprint than traditional data centers and can be set up nearly anywhere. Agencies can use it to extend existing data centers or as a standalone system for remote applications. The Cisco CDC can be ordered already provisioned with computing, networking, and storage resources and ready to be connected to power, chilled water, and the agency network. The main advantages of the Cisco CDC are low capital costs, rapid deployment, highly efficient power and cooling, COOP support, and short lead times compared to regular constructed sites.

Cisco Cloud Security Components

Five layers of security are needed to secure private and community clouds:

- **Cloud services security layer:** To protect applications and services residing in the cloud, each tenant needs a virtual firewall. A single Cisco ASA Adaptive Security Appliance acts as a services node and can be partitioned into multiple virtual firewalls called security contexts. The services node, inserted between the physical network and the virtual networks in the cloud, gives each tenant one or more separate security contexts for VLANs, virtual routing and forwarding (VRF), and firewall services.
- **Cloud edge:** To protect and secure the cloud service provider network and the cloud infrastructure itself, providers need firewall technologies, IDSs, and IPSs at the cloud edge.
- **Cloud data center edge:** This layer protects the cloud from threats originating from applications or the web. The Cisco IronPort™ S-Series Web Security Appliance (WSA) acts as a secure web gateway or software-as-a-service (SaaS) gateway, combining acceptable-use-policy (AUP) controls, reputation filtering, malware filtering, data security, and application visibility and control.

- **Security services layer:** Like traditional IT infrastructures, cloud architectures need physical firewalls, IDSs, and IPSs. Physical firewalls are still needed in cloud architectures because certain applications cannot be virtualized.
- **Secure virtual access layer:** Securing the virtual access layer requires Layer 2 through 7 security, especially as agencies virtualize more applications. Technologies to secure the virtual machine environment include a hardened operating system layer, hypervisor layer security, VMware VMsafe, and the Cisco Nexus 1000V Switch. In addition, Cisco Nexus 7000 Series Switches use VDCs and VRF to isolate each tenant's data as it travels through the cloud.

SaaS Cloud Options for Public-Sector and Community Clouds

An interesting side case for private cloud is a public-sector community cloud. A community cloud, which could be hosted by a public-sector institution for a common-interest community, would emulate a private cloud with the community as the end user. Examples include Cisco WebEx™ collaboration as a service cloud and ScanSafe Web Security services as a cloud.

Collaboration from the Cloud

According to Forrester Research, 7 out of 10 enterprises are investing in collaboration solutions[1] like unified communications. A majority of these organizations will outsource some or all of the software and hardware needed to enable their companies for collaboration. Gartner predicts that, "By 2012, 40% of enterprises will adopt a blend of cloud- and premises-based approaches to meet their UC needs."[1]

Community Clouds for Education

K-12 school districts facing budget shortfalls can free funds for teacher salaries and 21st-century learning by reducing IT costs. Similarly, colleges and universities can no longer depend on state funding and are looking abroad for collaborative research opportunities. Most educational institutions cannot afford a private cloud.

Multiple schools, colleges, and universities can participate in a community cloud. All member schools share infrastructure and operational resources, reducing costs. In higher education, community clouds also provide a framework for sharing research data, academic resources, and access to higher education networks. Real-world results of educational institutions that joined community clouds include the following:

- Two states with multiple school districts and more than 500,000 students saved more than US$1.5 million in the first 6 months.
- An education content provider for school districts reduced data center costs by 75 percent.
- Several universities worldwide use the National LambdaRail (NLR) Telepresence Exchange, a cloud service, for global collaboration. Average cost savings is 34 percent.

State and local government agencies can quickly implement community clouds using the Vblock and SMT architecture from Cisco, VMware, EMC and Netapp.

Sources: DigitalChalk Study (2010). E School News (August 2010), and Cisco Internal Education Study (2010)

To meet this increasing customer need for flexible deployment options, Cisco offers secure, rich collaboration solutions which can be deployed by an organization and delivered by certified Cisco partners in private cloud, public cloud or combination/hybrid deployment models.

Built on Cisco's proven strength in enterprise networking, virtualization, and the data center, the Cisco Collaboration Cloud Solutions offer superior security, resilience, scalability and quality of experience. Offering flexible deployment models and interoperability for communications and collaboration solutions can assist organizations in reducing the cost of IT operations while delivering, innovative solutions in rapid time to market.

Cisco Hosted Collaboration Solution

Building on existing hosted Cisco Unified Communications offerings, Cisco's Hosted Collaboration Solution enables highly specialized partners worldwide to deliver secure, integrated voice, messaging, presence/instant messaging (IM), mobile applications, web conferencing, and contact center services in flexible deployment models to the private and public sector.

With the Hosted Collaboration Solution open and interoperable design, organizations can choose the delivery model that best meets preference and business needs. The hybrid model provides ultimate choice, combining aspects across delivery models, a capability that is only possible with Cisco's open and interoperable approach.

[1] Gartner Predicts 2010: Video, Cloud and UC Services Loom Large in Enterprise Communications

Government Clouds Around the World

United Kingdom: G-Cloud

The government of the United Kingdom is establishing an onshore, private government cloud, called G-Cloud, providing IaaS, PaaS, and SaaS. Government customers will sign up for SaaS through an online applications store modeled after Apple's App Store. G-Cloud is helping the government achieve 10 strategic goals:

- Standardize and simplify the desktop.
- Standardize networks.
- Rationalize data centers.
- Commit to open source, open standards, and reusability.
- Make IT greener.
- Strengthen information security and assurance.
- Offer shared services, such as payroll, human resources management, and enterprise resource planning.
- Provide reliable project delivery.
- Manage suppliers.
- Transform IT-enabled business processes.

Sources of expected cost savings include reduction of the more than 10,000 software applications used in government, consolidation from 130 data centers to approximately 12, and increased server utilization.

Japan: Kasumigaseki Government Cloud

Japan's government wants to deliver government services more efficiently. As part of the effort, Japan's Ministry of Internal Affairs and Communications is building a massive cloud computing infrastructure to consolidate all government IT systems. Tentatively called the Kasumigaseki Cloud, the cloud will be built in stages, completing in 2015, with the goals of improving operational efficiency, reducing costs, and more rapidly introducing advanced government services. Instead of maintaining their own data centers, ministries will use shared resources, scaling up or down as needed.

In addition, because Cisco Unified Communications transparently brings disparate applications, devices, and environments together, organizations will be able to experience and deliver an integrated user experience over a variety of workspaces. Even if applications are delivered via cloud and premises infrastructure, all users will have a consistent experience.

Cisco WebEx Collaboration Cloud

Cisco's Webex Collaboration Cloud provides a real-time, global software-as-a-service (SaaS) cloud that delivers Cisco Webex collaboration applications with fast, reliable, and highly secure performance.

Public sector as well as private sector organizations utilize the secure WebEx Collaboration Cloud for email, instant messaging, and multimedia conferencing. The WebEx Collaboration Cloud is a private, global network owned and operated by Cisco. The secure infrastructure comprises multiple fully redundant data centers strategically located near major Internet access points around the world, and uses dedicated high-bandwidth fiber to route traffic around the world.

The WebEx Collaboration Cloud protects data confidentiality from end to end, using multilayered security:

- Protects physical sites and enforces stringent controls over personnel that administer and manage the service
- Safeguards message transport between desktop, mobile devices and the WebEx Collaboration Cloud
- Restricts access to user files and communications, authenticates users to determine appropriate privileges and service permissions, and enforces collaboration policies for each agency

In summary, Cisco Hosted Collaboration Cloud options provides government agencies flexibility in deployment options and the benefits of a secure, converged IP communications network without having to own, manage and maintain the hardware and software needed to support internal customer organizations.

ScanSafe Web Security

The ScanSafe SaaS cloud enables agencies to control and secure web traffic to reduce the risk of infections and attacks that could threaten government continuity. The ScanSafe Web Filtering service enables agencies to define the web-based content permitted to enter and exit the network. Another service, ScanSafe Web Security, uses dynamic, reputation- and behavior-based analysis to identify and block zero-day threats. It has been shown to stop 20 percent more malware than signature-based filtering solutions.

The ScanSafe SaaS platform consists of globally distributed data centers, highly parallel processing, multiple high-speed network providers, and extensive redundancy. Agencies that use ScanSafe SaaS receive SLAs with 99.999 percent uptime assurance.

Conclusion

Public-sector and federal government agencies can take their first steps with Cisco toward cloud computing and private cloud data centers. One should develop applicable and manageable use cases as initial points of entry into cloud computing. Start by identifying potential opportunities for cloud infrastructure. You should also consider other IT tasks such as the following to facilitate adoption of private cloud architectures:

- Map cloud architecture to enterprise architecture as part of an IT roadmap.
- Create a cloud task force or steering committee, with AMO and PMO functions to evaluate cloud adoption.
- Optimize the current IT environment first using an internal cloud services model and plan for federation of internal clouds with public and hybrid clouds.
- Pilot various services, both internally and in a community cloud.

We look forward to building the future of cloud computing with you and our ecosystem partners.

For More Information

- Cloud Powered by the Network: What Business Leaders Must Know: http://www.cisco.com/en/US/solutions/collateral/ns341/ns991/white_paper_c11-609220.pdf
- White paper about the Cisco cloud computing in the public sector: http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf
- Cloud Security Alliance: http://www.cloudsecurityalliance.org/
- Cisco Cloud Computing: http://www.cisco.com/go/cloud
- Cisco Unified Computing System: http://www.cisco.com/en/US/products/ps10265/index.html
- Unified fabric: http://www.cisco.com/en/US/netsol/ns945/ - ~in-depth
- Virtual Computing Environment coalition: http://www.cisco.com/en/US/netsol/ns1027/index.html
- SMT: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_dcVDDC.html
- VMDC: http://www.ciscosystems.com/en/US/solutions/collateral/ns340/ns517/ns224/ns836/white_paper_c11-604559.html
- Cisco WebEx services: http://www.cisco.com/en/US/products/ps10352/index.html
- ScanSafe: http://www.scansafe.com/services
- Cisco solutions for federal government: http://www.cisco.com/go/federal.

To arrange a demonstration of Cisco technologies at the Public Sector Center of Excellence, contact your local Cisco account team.

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 C11-617326-00 08/10