internet.com®

The Government's Plan for the Cloud

By Paul Rubens

Explore the Cloud First initiative launched by the U.S. federal government, and what it means to the network architect.

In late 2010, the U.S. federal government announced its "Cloud First" policy—a policy intended to ensure that the power of cloud computing is unleashed in as many federal agencies as possible.

During every IT procurement process, the Cloud First policy requires that federal agencies default to cloud-based solutions "whenever a secure, reliable, cost-effective cloud option exists." It is anticipated that the Cloud First policy will lead to increased IT resource utilization, improved flexibility and responsiveness, and reduced costs as part of a U.S. federal government drive to consolidate or close at least 40 percent of the 2,100 data centers it currently operates by 2015.

Pinning down exactly what is meant by cloud computing can be difficult; although if you are involved in IT, then you probably know it when you see it. 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 (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The five key characteristics that NIST identifies are:

- On-demand service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

When you think about cloud computing, you might imagine large-scale data centers operated by cloud service providers, offering one or more application services "down the wire" to customers located all over the world. This is the deployment model used by popular cloud computing services, such as Google's Gmail, but it is certainly not the only one.

In fact, NIST defines four deployment models that may be used by government agencies:

1. **Private cloud:** A cloud infrastructure that is used by a single agency. This infrastructure is usually located, owned, and managed in-house but may be located off premises and owned and managed by a third party.

2. **Public cloud:** A cloud infrastructure owned by a service provider that sells cloud services to anyone wishing to pay for it from one or more data centers.

3. **Community cloud:** Halfway between a public and a private cloud, a community cloud infrastructure is shared by a group or community of agencies that have shared objectives or concerns (such as security requirements, compliance considerations, or missions). The infrastructure may be owned and managed by one or more community members or by a third party.

4. **Hybrid cloud:** This is actually made up of two or more of the preceding cloud types, which use common technology—either standardized or proprietary. Because of this common technology, data and applications can be moved from one cloud to another when necessary. For example, applications can be moved from a private to a public cloud to provide extra capacity during periods of high demand.

The Implications for Network Architects

The impact of the Cloud First policy is likely to be very far reaching indeed: of the $80 billion that the U.S. federal government currently spends in IT, an estimated $20 billion is a potential target for migration to cloud computing solutions.

That means that if you are involved in network design for a government agency, then the Cloud First policy will likely be the catalyst for some profound changes to the way you plan your network infrastructure. That's because you will need to ensure that your entire existing and future network infrastructure is "cloud ready" and capable of supporting the different types of cloud deployments likely to be chosen as a result of the Cloud First policy: private, public, community, and hybrid clouds.

Aligning your agency with the government's Cloud First policy requires careful planning and a well thought out IT strategy. Brocade can help you with its next-generation networking products and its CloudPlex architecture: an open, extensible framework that enables you to build cloud-ready data centers using integrated compute blocks—servers, hypervisors, storage, and cloud-optimized networking in prebundled, preracked configurations with unified support—alongside your existing multivendor infrastructure.

Here are some of the key technologies that may play key roles in ensuring your networking infrastructure is cloud ready:

16 Gbps Fibre Channel

Clouds may require highly virtualized, high-performance storage environments to allow you to deal with the huge storage traffic flows that are generated as you provision and move dynamic applications and workloads around a cloud infrastructure. Fibre Channel continues to be the industry standard for storage networks, and industry-leading 16 Gbps Fibre Channel switches such as the Brocade 6510 and DCX 8510 Backbone can provide the storage bandwidth required.

Ethernet Fabric

Making your Ethernet network infrastructure ready for a private cloud is likely to involve some careful planning and reconfiguration. The reason is that today's traditional Ethernet networks employ relatively inefficient architectures that can be both complex to manage and costly to operate. A more sophisticated Ethernet fabric architecture can better support the demands of the cloud, because Ethernet fabrics are simpler to build and manage, very much more scalable, and, perhaps most importantly, designed specifically to meet the needs of highly virtualized and cloud-optimized data centers

Ethernet fabrics built using Brocade's VCS technology, available through the Brocade VDX family of data center switches, utilize available bandwidth much more efficiently than traditional Ethernet architectures that rely on Spanning Tree Protocol. VCS technology is also highly resilient and enables information sharing across fabric switches, providing application mobility and a way for your organization to scale and manage Ethernet fabrics as a single logical entity.

Converged Networking

Depending on the level of cloud deployments in your agency, it may make sense to switch to a converged networking approach: using an Ethernet-based network to carry both conventional LAN data traffic and encapsulated Fibre Channel frames transported using the Fibre Channel over Ethernet (FCoE) protocol. There are a number of reasons for this, including the cost of maintaining and managing separate network hardware, the problem of managing and configuring twice as many cables, and the complexity of including separate Fibre Channel host bus adapters as well as Ethernet interfaces on every server. Switches that employ Brocade's VCS technology will enable you to prioritize FCoE traffic (and iSCSI traffic for smaller SAN implementations) to ensure it received sufficient bandwidth and remains lossless.

100 Gigabit Ethernet

Large cloud deployments, such as those in community cloud facilities, can have very demanding networking connectivity requirements thanks to the sheer scale of operations and the volumes of data that need to be transported. Technology, such as Brocade's Ethernet fabric, and very high-density networking solutions, such as Brocade's MLXe 100 Gigabit Ethernet IP/MPLS routers, have been developed to ensure that your data center infrastructure can cope with the most demanding cloud computing environments.

The Cloud First policy is designed to help federal government agencies improve IT flexibility, maximize resource utilization, and minimize cost. Brocade technology can help ensure your cloud deployments are successful.