Hybrid Cloud

A hybrid cloud combines a standard data center with outsourced cloud computing. For many organizations, the hybrid cloud is the perfect migration to the cloud. In a hybrid architecture, the organization can run its applications and systems in its local data center and offload part of the computing to the cloud. This provides an opportunity for the organization to leverage its investment in its current technology while moving to the cloud. Hybrid clouds provide an opportunity to learn and develop the optimal cloud or hybrid architecture.

Applications for hybrid cloud include:

• Disaster recovery – Run the organization computing locally, with a backup data center in the cloud.

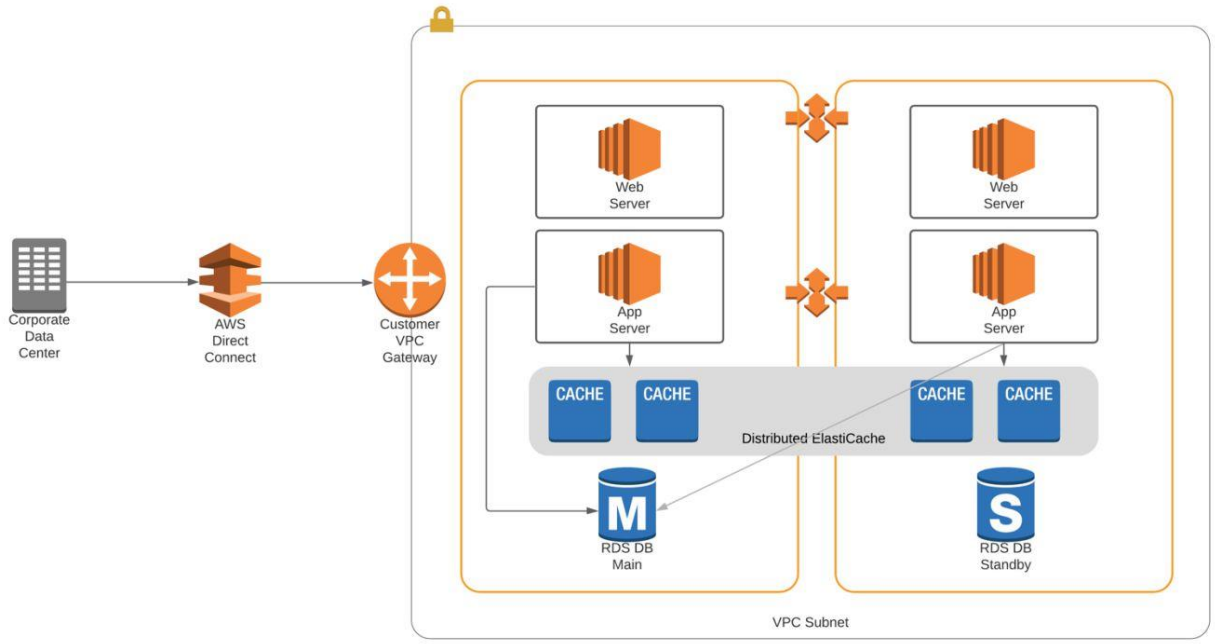
• On-demand capacity – Prepare for spikes in application traffic by routing extra traffic to the cloud.

• High performance – Some applications benefit from the reduced latency and higher network capacity available on-premises, and all other applications can be migrated to the cloud to reduce costs and increase flexibility.

• Specialized workloads – Move certain workflows to the cloud that require substantial development time, i.e., machine learning, rendering, transcoding.

• Backup – The cloud provides an excellent means to back up to a remote and secure location.

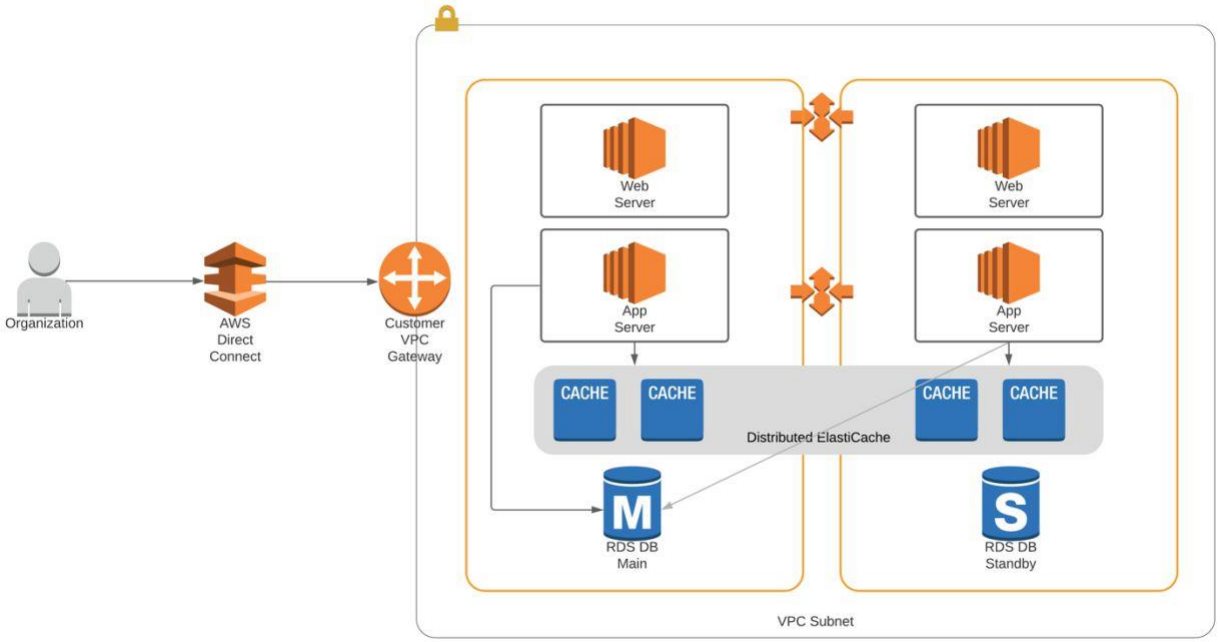
The diagram below shows an example of a hybrid cloud computing environment.



Pure Cloud Computing Environment

In a pure cloud computing environment, all computing resources are in the cloud. This means servers, storage, applications, databases, and load balancers are all in the cloud. The organization is connected to the cloud with a direct connection or a VPN connection. The speed and reliability of the connection to the cloud provider will be the key determinant of the performance of this environment.

The diagram below shows an example of a pure cloud computing environment on the AWS platform



A pure cloud computing environment has several advantages:

Scalability – The cloud provides incredible scalability.

Agility – Adding computing resources can occur in minutes versus weeks in a traditional environment.

Pay-as-you-go pricing – Instead of purchasing equipment for maximum capacity, which may be idle 90 percent of the time, exactly what is needed is purchased when needed. This can provide tremendous savings.

Professional management – Managing data centers is very complicated. Space, power, cooling, server management, database design, and many other components can easily overwhelm most IT organizations. With the cloud, most of these are managed for you by highly skilled individuals, which reduces the risk of configuration mistakes, security problems, and outages.

Self-healing – Cloud computing can be set up with health checks that can remediate problems before they have a significant effect on users.

Enhanced security – Most cloud organizations provide a highly secure environment. Most enterprises would not have access to this level of security due to the costs of the technology and the individuals to manage it.

Connections to the Cloud

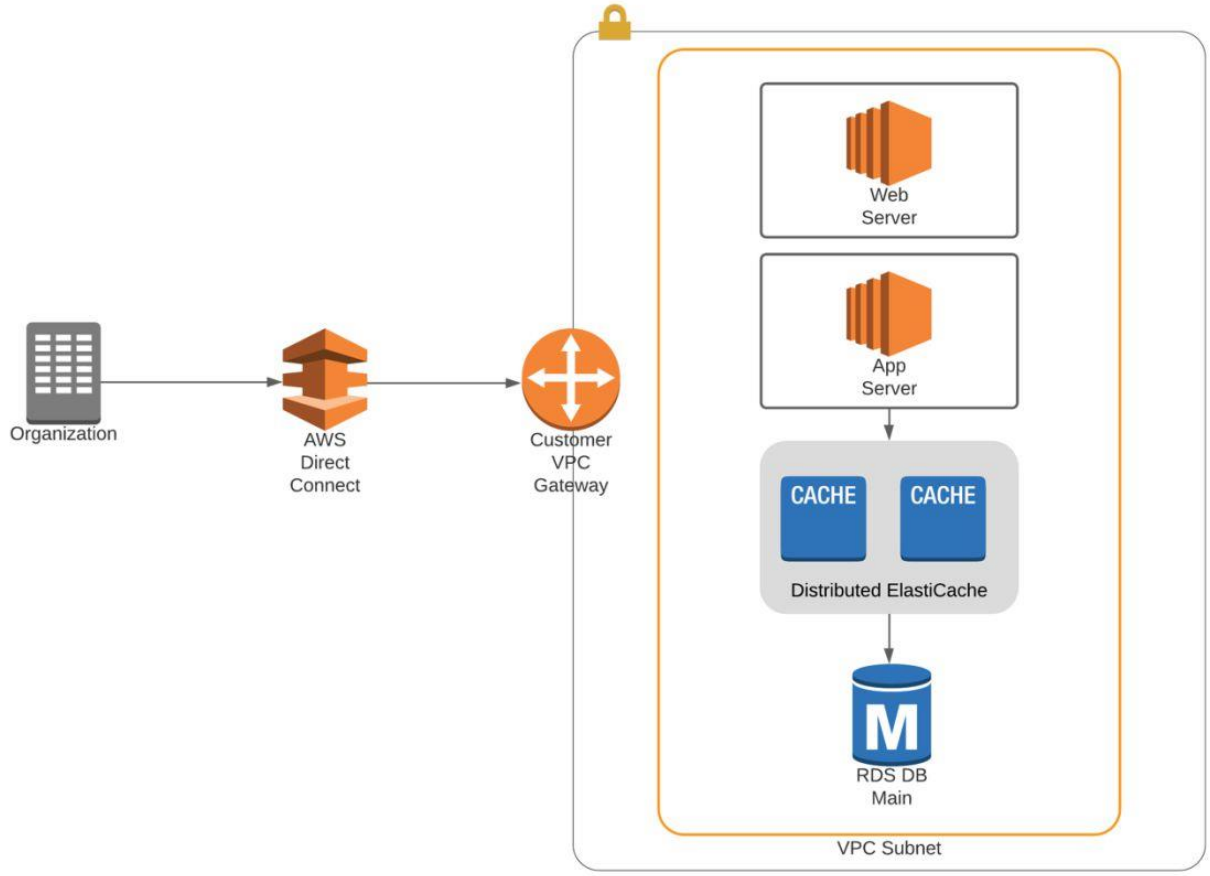
If an organization moves its computing environment to the cloud, then the connection to the cloud becomes critical. If the connection to the cloud fails, then the organization can no longer access cloud resources. The performance needs and an organization's dependency on IT will determine the connection requirements to the cloud.

For most organizations, getting a "direct" connection to the cloud will be the preferred method.

A direct connection is analogous to a private line in the networking world because it is effectively a wire that connects the organization to the cloud. This means guaranteed performance, bandwidth, and latency. As long as the connection is available, performance is excellent. This is unlike a VPN connection over the internet, where congestion anywhere on the internet can negatively affect performance.

Since network connections can fail, a direct connection is generally combined with a VPN backup over the internet. A VPN can send the data securely over the internet to AWS. A VPN provides data security via encryption and permits the transfer of routing information and the use of private address space. VPNs work by creating an IP security (IPsec) tunnel over the internet

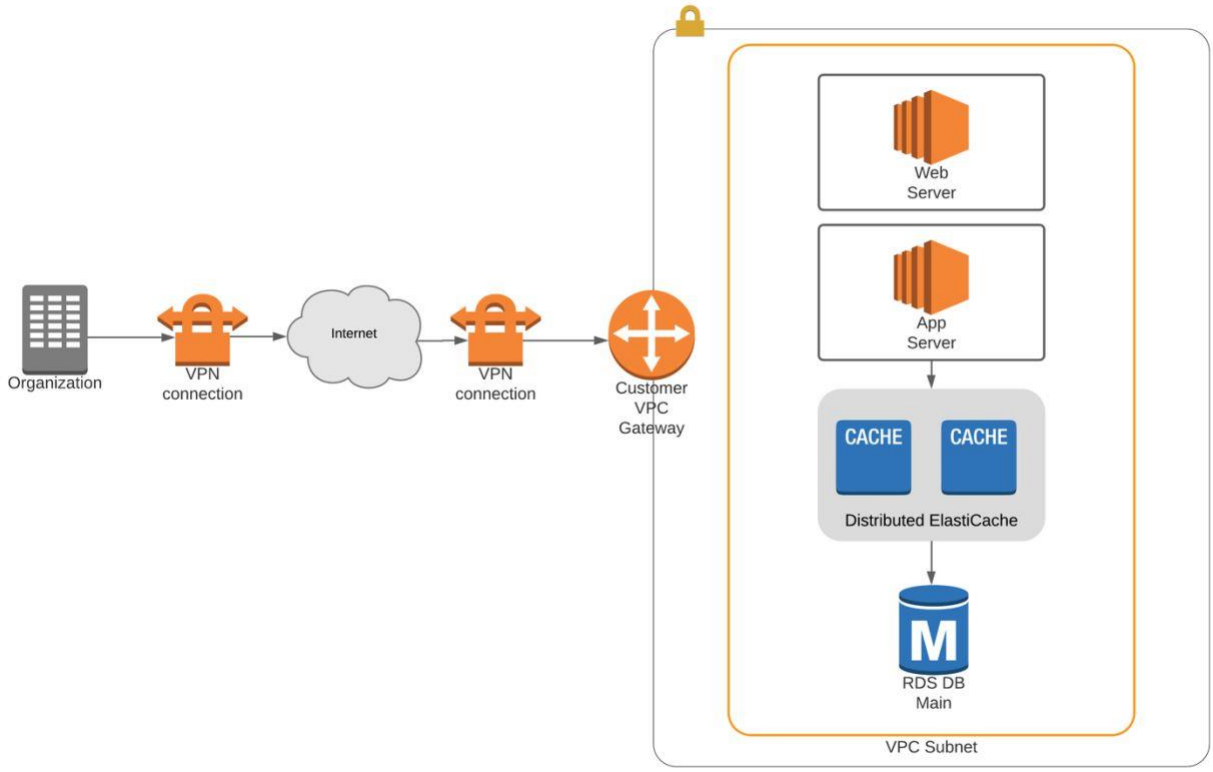
The diagram below shows an example of a direct connection to the AWS platform.



VPN Connection to AWS

The simplest and cheapest means to connect to AWS is a VPN. A VPN provides a means to "tunnel" traffic over the internet in a secure manner. Encryption is provided by IPsec, which provides a means to provide encryption (privacy), authentication (identifying of the user), data authenticity (meaning the data has not been changed), and non-repudiation (meaning, the user can't say they didn't send the message after the fact). However, the problem with VPN connections is that while the connection speed to the internet is guaranteed, there is no control of what happens on the internet. So, there can be substantial performance degradation based upon the availability, routing, and congestion on the internet. VPN-only connections are ideal for remote workers and small branches of a few workers, where if they lose connectivity, there will not be significant costs to the organization.

The diagram below shows an example of a VPN connecting to the AWS platform



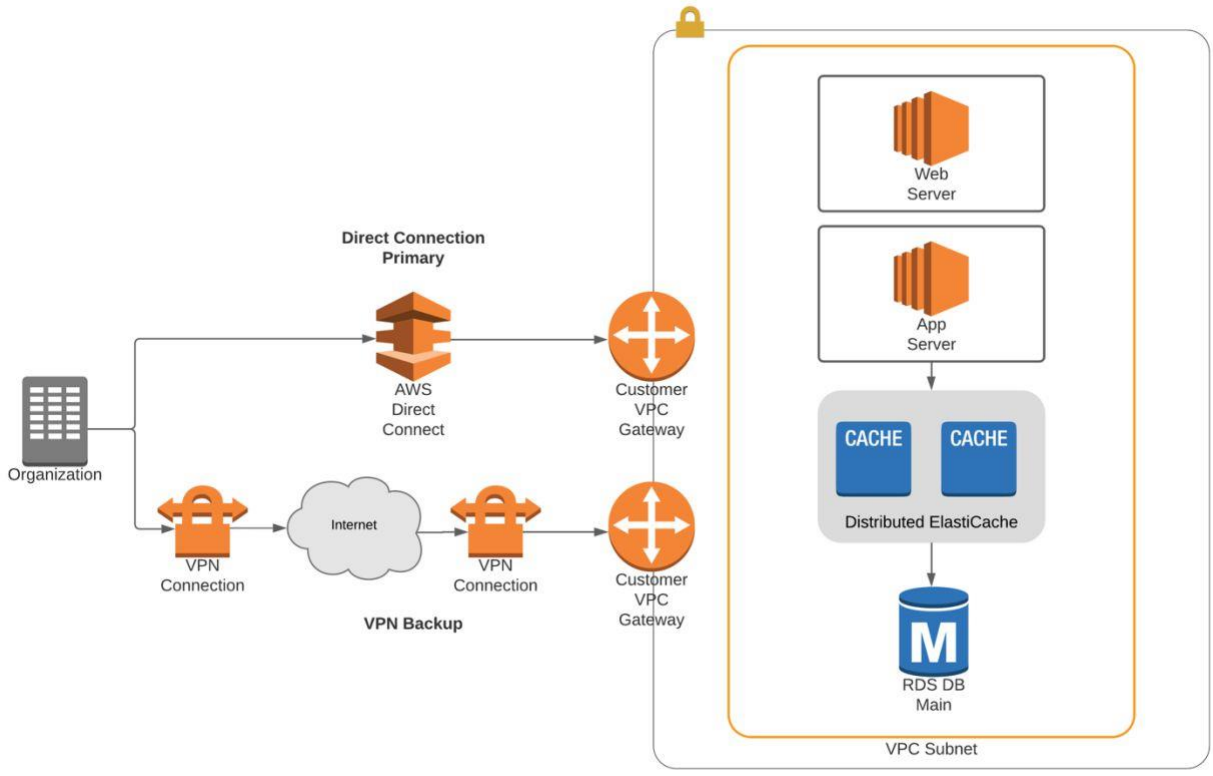
High-Availability Connections

Connecting to the cloud with high availability is essential when an organization depends upon technology.

The highest availability architectures will include at least two direct connections to the cloud.

Ideally, each connection is with a separate service provider, a dedicated router, and each router connected to different power sources. This configuration provides redundancy to the network connection, power failures, and the routers connecting to the cloud. For organizations that need 99.999 percent availability, this type of configuration is essential.

For even higheravailability, there can be a VPN connection as a backup to the other direct connections.



High Availability at Lower Costs

A lower cost means to achieve high availability is to have a dedicated connection and a VPN backup to the cloud. This will work well for most organizations, assuming they can tolerate reduced performance when using the backup environment.

Storage Options on the AWS Cloud Platform

There are several storage options available to AWS cloud computing customers. They are: AWS Simple Storage Service (S3), Elastic Block Storage, Elastic File System, Storage Gateways, and WorkDocs.

In traditional data centers, there are two kinds of storage—block storage and file storage. Block storage is used to store data files on storage area networks (SANs) or cloud-based storage environments. It is excellent for computing situations where there is a need for fast, efficient, and reliable data transportation. File storage is stored on local systems, servers, or network file systems.

AWS Primary Storage Options

In the AWS cloud environment, there are three types of storage: block storage, object storage, and file storage.

Block Storage

Block storage places data into blocks and then stores those blocks as separate pieces. Each block has a unique identifier. This type of storage places those blocks of data wherever it is most efficient. This enables incredible scalability and works well with numerous operating systems.

Object Storage

Object-based storage differs from block storage. Object storage breaks data files into pieces called objects. It then stores those objects in a single place that can be used by multiple systems that have network access to the storage. Since each object will have a unique ID, it's easy for computing resources to access data on file-based storage. Additionally, each object has metadata or information about the data to make it easier to find when needed.

File Storage

File storage is traditional storage. It can be used for a systems operating system and network file systems. Examples of this are NTFS-based volumes for Windows systems and NFS volumes for Linux/UNIX systems. These volumes can be mounted and directly accessed by numerous computing resources simultaneously