ISSN:0975-9646

Cloud Network: Integration of Cloud Computing and Virtualization with Network

Puram.Pradeep Kumar, R.Sai Krishna,.Kishor Kumar, Naini.Shekar Reddy, M.Ramesh

VITS Engineering College, KarimNagar.

Abstract- In cloud computing environment (cloud) typically compute, storage and software resources are offered no-demand via IaaS (Infrastructure as a Service), PaaS (Platform as a Service) or SaaS (Software as a Service) services. With proper integration of Cloud computing and virtualization with network much richer and differentiated Cloud services can be offered. A network is an integral part of a Cloud connecting various segments (multiple DCs, CSC to CSP, etc) of a Cloud. But network can be further integrated into cloud by supporting relevant Cloud features in the network itself. While there are many Cloud-ready features that can be supported, some of the important features are on-demand network management functions and interfaces, VM-aware networking, and layer two (L2) and layer (L3) scaling (such as IETF LISP and TRILL or Cisco Fabric Path).

Keywords: Cloud Computing, Network, VM-aware networking.

1. INTRODUCTION:

As stated in[1] a Cloud Service Provider (CSP) offers cloud services out of one or more DC's, where compute, storage ,and network resources are offered on-demand to cloud service consumers(CSC).the infrastructure resources are offered via a service called the Infrastructure as a service (IaaS),where a CSC can acquire and release resources on –demand and elastically (grow or shrink at will)and pay for the services or resources per use .in addition to the infrastructure resource, the software resources are also offered via platform as a service (PaaS) and software as a service (SaaS) in the same elastic, on-demand and pricing models. In the case of PaaS, software development and testing platforms and software middleware components are offered as on-demand resources. In the case of SaaS, full-fledged application products are offered as on-demand resources.

A network is an integral part of a cloud connecting various segments (multiple DC's CSC to CSP, etc.) of a cloud. But network can be further integrated in to cloud by supporting relevant cloud features in the network itself. While there are many cloud –ready features that can be supported, some of the important features are on-demand network management functions and interface,VM-aware networking, and layer two (L2) and layer (L3) scaling (such as IETF LISP and TRILL or Cisco fabric path).We will not cover L2 scaling in this paper.

2. CLOUD COMPUTING

Cloud Computing [2] is a style of computing which must cater to the following computing needs:

2.1 Dynamism

Your business is growing exponentially. Your computing need & usage is getting bigger with every passing day. Would you add servers & other hardwares to meet the new demand? Assume, Recession is back & your business is losing customers. The servers & hardwares you added during last quarter's peak season is now idle. Will you sale them? Demand keeps on changing based on world/regional economy, sometimes seasonal traffic burst as well. That's where Cloud Computing comes to your rescue! You just need to configure & your provider will take care of fluctuating demand.

2.2 Abstraction

Your business should focus on your core competency & should not worry about security, OS, software platform , updates and patches etc. Leave these chores to your provider. From an end users perspective, you don't need to care for the OS, the plug-ins, web security or the software platform. Everything should be in place without any worry.

2.3 Resource Sharing

Resource Sharing is the beauty of Cloud Computing. This is the concept which helps the cloud providers to attain optimum utilization of resources. Say, a company dealing in gifts may require more server resources during festive season. A company dealing in Payroll management may require more resources during the end or beginning of the month[2].

The cloud architecture is implemented in such a way that it provides you the flexibility to share application as well as other network resources (hardware etc). This will lead to a need based flexible architecture where the resources will expand or contract with little configuration changes.

3. CLOUD SERVICES

They are divided into 3 stacks

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

3.1 Infrastructure as a Service (IaaS)

This is the base layer of the cloud stack[2]. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization.

Fig. 1 Three Layers of Cloud Computing.

3.2 Platform as a Service (PaaS)

Now you don't need to invest millions of $$$ to get that development foundation ready for your developers. The PaaS provider will deliver the platform on the web, and in most of the cases you can consume the platform using your browser, i.e. no need to download any software. It has definitely empowered small & mid-size companies or even an individual developer to launch their own SaaS leveraging the power of these platform providers, without any initial investment.

1. *PaaS Layers*
2. *Cloud OS*
3. *Cloud Middleware*

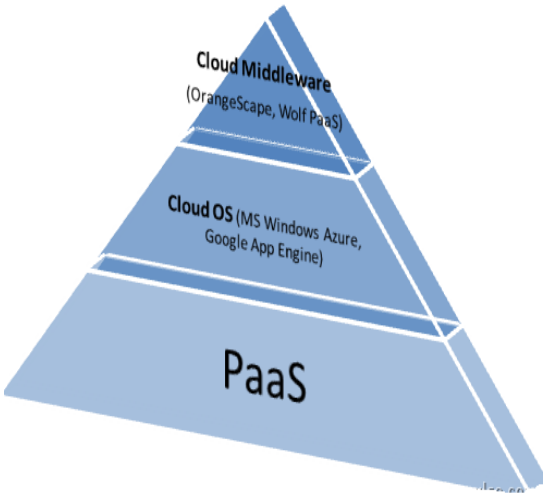

Fig.2 PaaS Layers

3.3 Software as a Service (SaaS)

This is the Top most layer of the cloud computing stack[2] - directly consumed by end user i.e. SaaS (Software as a Service). On-Premise applications are quite expensive, affordable only to big enterprises. The Cause On-Premise applications had a very high upfront CapEx(Capital Expenditure); which results in a high TCO (Total Cost of Ownership). On-Premise apps also require a higher number of skilled developers to maintain the application. In its current avatar SaaS is going to be the best bet for SMEs/SMBs (Small & Mid size businesses). Now, they can afford best software solution for their business without investing anything at all on the infrastructure or development platform or skilled manpower. The only requirement for SaaS is a computer with browser, quite basic. SaaS is a recurring subscription based model delivered to customer on demand – Pay as use.

Best SaaS Examples

1. SalesForce
2. CRM Google Apps
3. ZOHO Support
4. Deskaway
5. ImpelCRM
6. Wipro w-SaaS

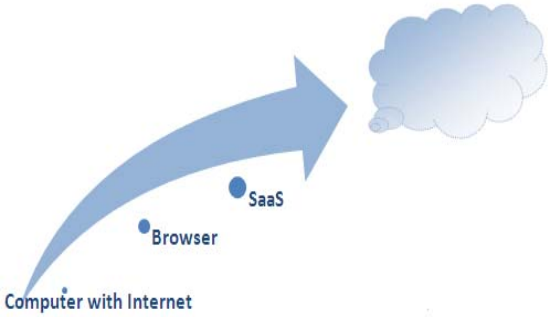

Fig.3 SaaS (Software as a Service).

4. ON –DEMAND NETWORK MANAGEMENT FUNCTIONS

Typically any feature required of a network is statically (a priori) configured by a network management system (NMS). But in on-demand cloud [3][4]it may not be known beforehand when, what and how much of network resources are to be configured. It is possible to oversubscribe, but

1. It beats the purpose of on-demand cloud with waste of resources.
2. CSCs will not be willing to pay for resources that otherwise are not used.
3. In a cloud everything should be invoked, configured, provisioned and monitored on-demand (if not ,it is not a cloud). Resources may be oversubscribed or aggregated in to a pool, but individual CSC requests should be realized (that includes automatic invocation of network functions) on-demand end-to-end (possibly from an oversubscribed resource pool). It is obvious that there is need for network or network management functions and relevant interfaces out of network or network management systems that can be invoked on-demand to realize a CSC request.

Note that network or network management functions include not only configuration and provisioning, but also creation or deletion of (virtual) network resources. When

we refer to network function Invocation, it refers to configuration / provisioning (de-configuration/de-provisioning) of network policies on network resources or creation (deletion) of network resources.

A few use-cases requiring on-demand network management functions are as follows:

1. When compute and storage resources are required or released on-demand, the relevant network functions have to be invoked on-demand.
2. When resources move, the relevant network policies and states have to be automatically moved and configured at new locations.
3. When network resources (such as virtual firewall, load balancer, bandwidth or QOS) themselves are requested by a CSC, on-demand, network functions have to be invoked on-demand. Network resources (such as virtual firewall) can also be requested (indirectly) as part of other requests (see the app-tier example below).
4. When certain wide area network oriented service, such as hybrid cloud service is requested by a CSC on-demand, a number of network functions' have to be invoked on-demand (including for example, VPN related network functions). A hybrid cloud service allows an enterprise (intranet, DC or private cloud) seamlessly extend in to public clouds on-demand. The hybrid cloud service requires the capability of on-demand network functions supported end-to-end (from CSC intranet, DC or private cloud via the MAN/WAN to cloud resources residing in CSPDCs).

5. VM-AWARE NETWORKING

Visualization of resources is very important in an environment like cloud where resources are acquired or released on-demand[5][6]. As servers are consolidated as virtual servers or machines (VM) on a physical machine, the networking or the switches connecting the VMs and physical servers should be VM-aware as follows:

5.1 Virtual switch

In a non-VM environment a server is connected to an access switch with rich set of capabilities[5]. A network manager can apply rich set of network policies on those switches to manage and control traffic to/from the server. In a VM environment the leaf access switch moves to the hypervisor as software-based virtual access switch (VAS), which obviously has to support network capabilities that are VM-aware.but a typical VAS is very limited in networking capabilities compared to what are supported in hardware access switches (which network managers are familiar with).the software-based VAS can be augmented with the rich capabilities supported in hardware –based access switches for effective VM-aware networking. The Cisco nexus 1000v in one such VAS. The VM-aware networking together with rich switch capabilities mentioned above can also be supported in hardware –based solutions incorporating features specified in IEEE 8021.1Q and 802.1Qbg.

5.2 On-demand network function invocation

In a cloud a VM is provisioned on-demand as results of a request by a CSC. The VM provisioning should trigger following network functions on-demand:

5.3 Creation of switch side virtual port:

As stated in [6] the switch and its ports are virtual, the virtual port or interface (VIF or VETH) connecting to the VM (VNIC) has to be created on-demand.

Association or configuration of network policies (port-profile in Cisco nexus 1kv term) on VIF or VECH on-demand.

It is also possible to create multiple instances of VAS (or VEM virtual Ethernet Module in Cisco Nexus 1kv term) on-demand.

5.4 VM or workload migration or mobility:

As a VM or workload moves to a new physical server either hot or live (such as VMware v Motion) or cold, the VIF at the destination has to be created automatically and network policies configured on it on-demand[7].

5.5 VM-aware APP-tier security

The web, application and database servers in an enterprise DC are deployed in a tired architecture (app-tier) [1],where the web server is placed on the DMZ segment of the DC network, application servers on the access segment (connected to the access switches)and DB servers on the access and storage segments (SAN/NAS) of the DC network . each of the segments (tiers)may be firewalled from each other with proper security policies (for example ,a web server may not be allowed to communicate directly with a DB server).

A CSC may request creation of such an app-tier in the cloud, where each of the servers and firewalls in the tier will be virtualized and provisioned on-demand, as a result the firewall or network or network security policies have to be configured on-demand.in addition, a CSP has to support multiple tenants over the same physical resources in the CSP cloud DC. Hence app-tiers of tenants have to be isolated from each other.

It obvious that in this case VM-aware networking should include VM –aware APP-tier firewalling or security policy support. The Cisco nexus 1kVSG (virtual security gateway), for example, supports this.

6. SCALING CSP L3 NETWORK

A CSP operating and managing a cloud[1] with many CSC tenants with each tenant acquiring resources (VM or storage) at any scale encounter following issues

6.1 Addressing

Each resource is assigning an ID: IP address, URI, and DNS name, many of the resources will be assigned private IP addresses. But if any resource has to be public facing (via internet or SP private MAN/WAN), then it will be assigned either a public IP address or public VIP (virtual IP) of a load balancer to which the resources is

assigned (either on-demand by a CSC or by the CSP itself).With many tenants served by a CSP the number of such public facing resources or IP addresses can be huge. Mobility and location independent addressing in cloud: Resources (VMs) may be moved around or provisioned in any location (CSC controlled or not) and objects (such as cloud storage objects) may be cached in different locations .But the resources should be accessible (by the CSCs) in a transparent manner (via location independent addressing).

In order to deal with huge scale it is obvious that proper schemes and infrastructure support for scalable cloud addressing and routing is needed. A CSP will be able to better scale manage cloud resources and associated routing if following is addressed:

IP address or prefixes of the dynamically changing public – Facing resources are taken off the core routing domain (internet DFZ: default free zone or SP private MAN/WAN core).

Identifier of these resources can be of any format (not just IP address) and location independent.

The IETF locater /ID separation protocol (LISP) has been designed to scale internet routing. But it can be useful in other areas, such as cloud where L3 scalability, as discussed above is required. The basic premise behind LISP is to separate the addressing domain or ID of endpoints (EID) from that of routing domain or locaters (RLOC).An IP address of an endpoint in the current internet architecture covers both the address domains in a single addressing scheme. In a LISP based network the core routing, domain knows how to route to an RLOC, which in turn knows how to route to an EID.

In a cloud environment a public facing resource can be endpoint with (LISP) EID, which is assigned to public facing RLOC (which is fewer in numbers), thus addressing the scalability, mobility and location independent addressing issues discussed above.

CONCLUSION:

In this paper we have explained that with proper integration of Cloud computing and virtualization with network much richer and differentiated Cloud services can be offered. As we know that network is an integral part of a Cloud connecting various segments (multiple DCs, CSC to CSP, etc) of a Cloud. The network can be further integrated into cloud by supporting relevant Cloud features in the network itself. We have many Cloud-ready features that can be supported, some of the important features are on-demand network management functions and interfaces, VM-aware networking, and layer two (L2) and layer (L3) scaling (such as IETF LISP and TRILL or Cisco Fabric Path).

REFERENCES

[1] Cloud Networking: www.csiindia. org/c/ document_library /get_file?uuid=745ba261.[2] Cloud Computing for Beginners http://www.techno-pulse.com/ Visit Techno-Pulse to learn more about Cloud Computing

[3] A. Clemm: Network Management Fundamentals. CiscoPress, 2006: www.cisco.com

[4] Fingerpointing, Frustrated Network Engineers, and the Application Performance Blame Game: www.cisco.com

[5] Cisco VN-Link Virtual Machine-Aware Networking www.cisco.com/en/US/prod/.../at_a_glance_c45-532467.pdf

[6] BLADE Network Technologies, “VMready : A Virtualization Aware Network Switch”,

[7] Live Migration of Virtual Machines www.portal.acm.org VMWare, Inc. VMWare Virtual Center Version 1.2 User’s Manual.2004.