LGURJCSIT
Volume No. 1, Issue No. 4 (October- December), pp. 13-19

AN OVERVIEW ON HUAWEI MANAGEONE SERVICES

Shan-e-zahra, Sabir Abbas

Abstract: Huawei ManageOne is a server farm administrative arrangement design for disentangled administration and dexterous operations. It bounds administration of different server and gives integrated end-to-end management solutions for incremented operations and managerial services and overall performance of data centers. ManageOne provides different efficient network services as discussed in this paper.

Keywords: *cloud computing, ManageOne services, Huawei network.*

1. INTRODUCTION

The ManageOne includes two components: service center and operation center. The service center is responsible for the service provisioning. The operation center is responsible for maintenance and monitoring. The IaaS resource pool is provided by FusionSphere OpenStack and supports the VRM and VMware. In multi-open stack scenarios, only one Key Stone is supported. BC&DR products in the disaster recovery solution provide backup and disaster recovery services for VMs. The backup services support only disk backup. The disaster recovery services support VM disaster recovery, and is applied for online and provisioned manually. The fusion insight resource pool provides big data services, including

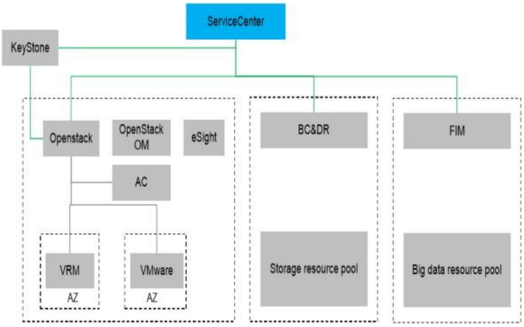

Figure.1. Manage One Operation Architecture

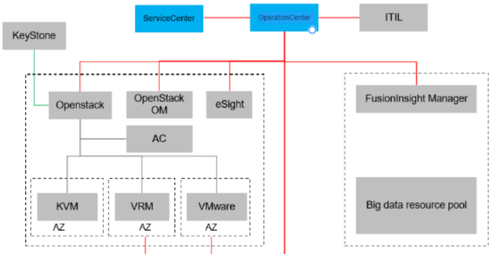

Figure.2. Manage One O&M Architecture

[1,2] Lahore Garrison University

HDFS, Hbase, Spark, Hive, and MapReduce. These services are automatically provisioned [1].

The ManageOne includes two components: service center and operation center. The service center is responsible for service provisioning. The operation center is responsible for maintenance and monitoring. The eSight monitors physical devices in DCs. The OpenStack, OM, VRM, and VMware monitor virtual devices in DCs. The OperationCenter summarizes monitoring information about physical and virtual devices, and provides unified views. The Fusion Insight resource pool provides big data services.

2. MANAGE ONE SERVICES

2.1 VPC (Virtual private cloud)

VPC provides a logical isolated network architecture that enables users to use VMs in a user-defined virtual network. You can totally control your own virtual network environment, including setting IP address, creating networks, and configuring security policies. It easily defines the network configuration of VPCs. For instance, a directed system for getting Internet web server and back-end frameworks, are the example of database or application servers. You can also use the access control list (ACL) to manage VM access on each network. Arrange source organize address interpretation (SNAT) for VMs on the steered system to empower them to get to the Internet [2].

a. VPC Functions

Use the ACL to control network access. Use the application specific packet filtering (ASPF) function to filter application-layer packets. Allocate multiple IP addresses for the VMs in the VPC and enable them to connect to multiple defined networks. Configure one or multiple Amazon elastic IP address to be reachable to a VM in the VPC so, this VM might be accessible from the Internet. Signing in to VMs effortlessly utilizing VNC, similarly as they are running in infrastructure. Empower SNAT for systems in the VPC with the goal that your VMs can get to the Internet whenever. Utilize IPSec VPN to interface the VPC and the infrastructure. A VPC provides a secure, isolated network environment in a VDC. Customize virtual networks that serve as traditional networks in the VPC and also provide advanced network services, including elastic IP addresses and SNAT to keep up with service deployment requirements.

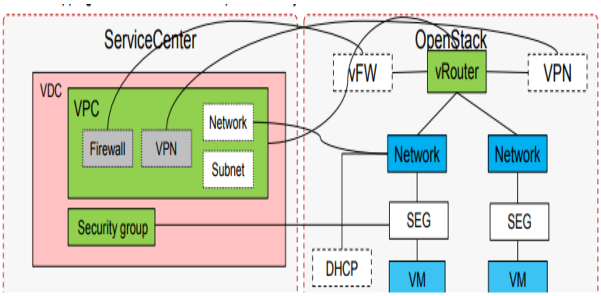

Figure.3. VPC Network

The mappings between a VPC and Open Stack objects are as follows:

A VDC administrator can create a VPC and security groups in a VDC.

1. A Router, not associated with outer systems, will be synchronously made in Open Stack when you make a VPC.
2. After applying for a switch in a VPC, you can apply for VPNs, firewalls, systems, and subnets. The Subnets can empower the DHCP work [2].

b. Feature configuration

1. A VPC corresponds to a Router in Open Stack. The VPC is successfully created, indicating that a Router, not associated with external networks, is created at the underlying layer. If the Router is associated with an external network, the VRF cannot be created on a physical switch [2].
2. VPCs related with QoS details and it is utilized to confine the inbound and outbound system movement rates. QoS determinations should be designed in Fusion Sphere Open Stack OM.
3. NTP server information configured in a VPC

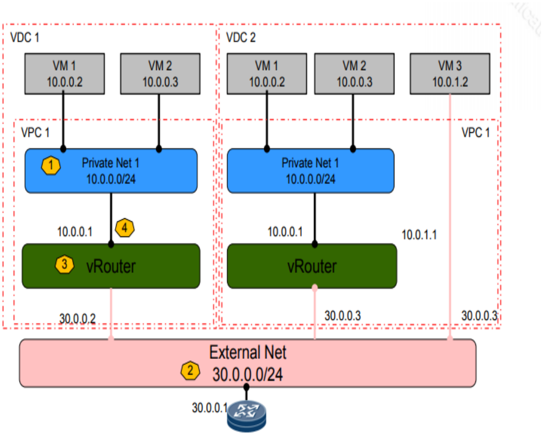

Figure.4. Network Service

2.2 Network Service — Network

Internal network:

Private networks can be made in a VPC[2], for example, Private Net 1, 10.0.0.0/24. It is suggested that private systems in various VPCs don't cover.The private systems in various VPCs cover, correspondence between VPCs is influenced. Private systems have internal systems,e.g. Private Net 1 in VDC 1 and Private Net 1 and Private Net 2 in VDC 2. IP deliver doling out mode to DHCP or Manual when you have to make a network.

2.3 Routed Network

Routed network gives VLANs and layer 3 gateways. All routed networks in a VPC can speak with each other. The directed system is utilized to associate with outside systems.

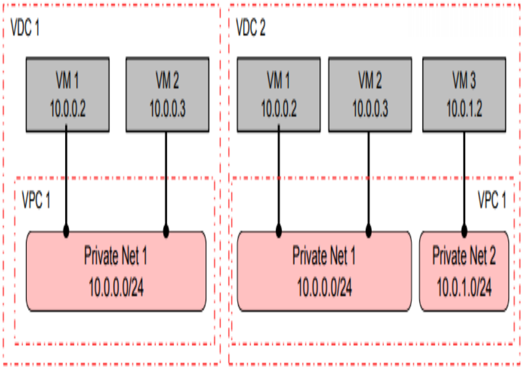

Figure.5. Routed Service

Routers can be created in a VPC and are associated with private networks in the same VPC. After the association is successful, the private networks become routed networks. For example, after Private Net 1 in VDC 1 and Private Net 1 in VDC 2 are associated with Routers in VDC 1 and VDC 2, the two private networks become routed networks [3].

2.4 Direct Network

Directed network interfaces VMs straightforwardly to outside systems. The passages and switches of an immediate System change the VDC administration arrange plane.

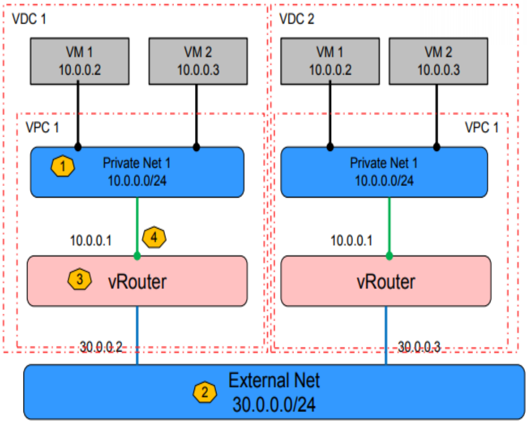

Figure.6. Directed Network

Switches are related to direct networks, diverse VPCs can speak with each other. External Net 30.0.0.0/24 in the figure is an immediate system. The VM connected in an immediate system can interface with outside systems. IP address can be stuck an immediate system and scrape the IP deliver to a VM port with the goal that can get to the VM from an open system [4].

2.5 Network Service — Router

A switch can be utilized to make a routed network. Routed network in a VPC can speak with each other. VMs in a steered system can get to an open system utilizing the flexible IP address and SNAT.

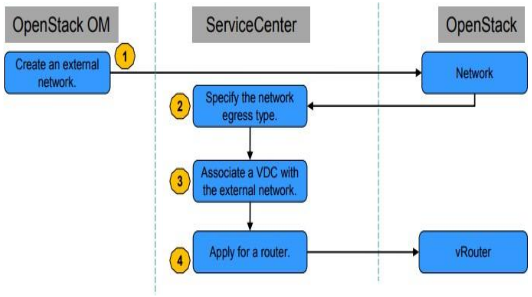
OpenStack OM
ServiceCenter
OpenStack
Create an external network.
1
Network
2
Specify the network egress type.
3
Associate a VDC with the external network.
4
Apply for a router.
vRouter

Figure.7. Router Service

2.6 Network Service — Elastic IP Address

A flexible IP address is an open IP deliver that is bound to a VM on a steered arrange, making administration VMs in a VPC available to outside administrations utilizing settled public IP addresses.

2.7 Network Service — SNAT

Source network address interpretation (SNAT): If an inside IP deliver starts an association with the administrations on people in general system, the passage on the switch or firewall deciphers the private IP address into an open IP address. This procedure is known as SNAT, which applies to access to open systems utilizing shared internal IP addresses [4][5].

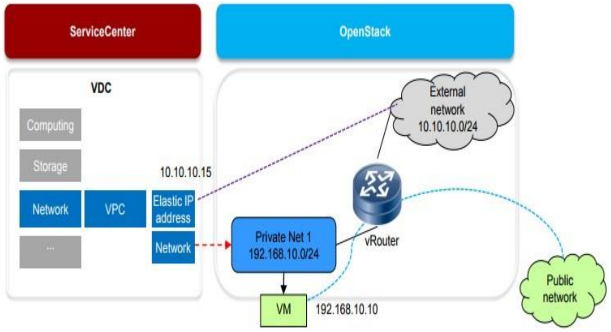

Figure.8. Elastic IP Address

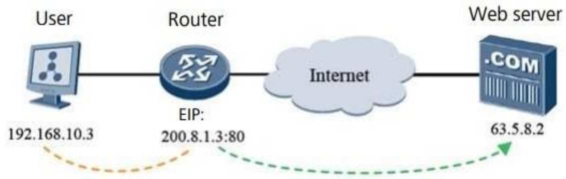

Figure.9. SNAT Services

2.8 Network Service — Firewall

A physical firewall can be separated into various virtual firewalls. Each logical firewall can work as a free firewall gadget to serve a venture by giving a private system, guaranteeing information security, and augmenting firewall asset use. Virtual firewalls are given by physical or programming firewalls.

2.9 Network Service — IPSec VPN

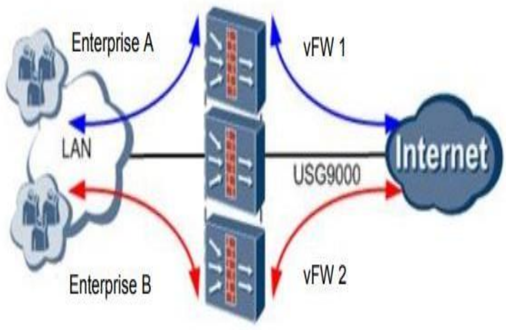

Figure.10. Firewall Services

A VPN is a virtual particular system set up on a public network and is used to transmit private system activity. A physical system can be consistently separated into different secludes systems, this guarantees secure and reliable system association without changing the network [6].

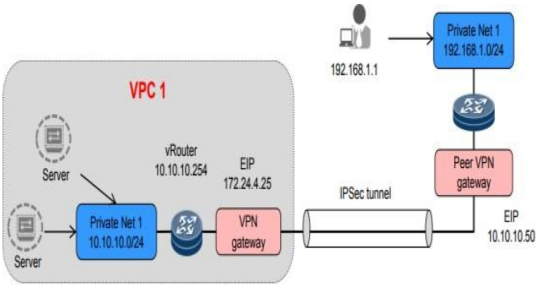

Figure.11. IPSec VPN services

2.10 Network Service — VLB

Load adjusting is a system benefit which disperses movement of various servers running a similar application [7]. The VLB function is implemented using the F5 load balancer.

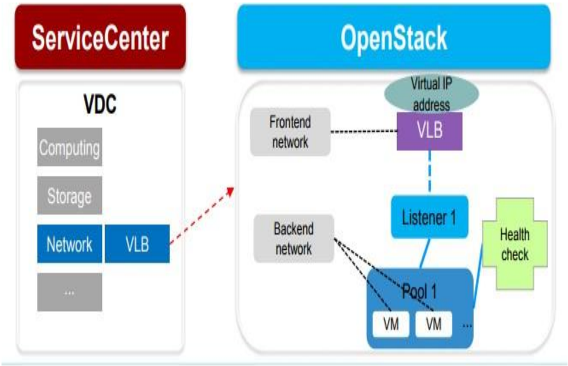

Figure.12. VLB services

2.11 Network Service — Security Group

A security bunch works as a virtual firewall for cloud hosts to control the inbound and outbound system data and just enables approved messages to pass. VMs in a similar security gathering might be conveyed to different servers and can speak with each other. VMs in various security bunches can't speak with each other as a matter of course. You can arrange a predetermined security gather manage to permit VMs in various security gatherings to speak with each other.

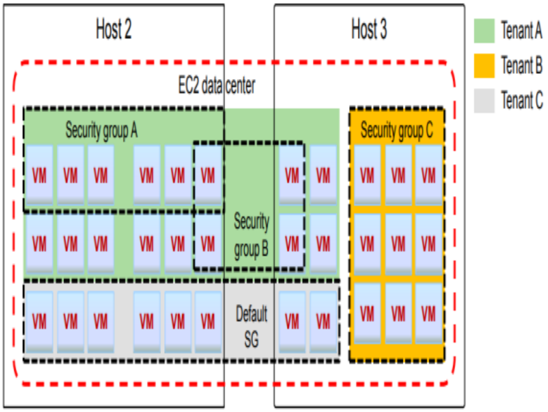

Figure.13. Security Group services

3 CONCLUSION

Data center virtualization allows multiple virtual machines (VMs) and applications to run on one physical server. This technology decouples the services from IT hardware resources and changes the traditional stove-pipe IT structure in which one application occupies one physical server. The discussed ManageOne services like VPN routed network & others provides efficiency to the users.

4 REFERENCES

[1] Bamiah, M. A., & Brohi, S. N. (2011). Exploring the cloud deployment and service delivery models. *International Journal of Research and Reviews in Information Sciences*.

[2] Griffin, D. P., & Georgatsos, P. (1995). A TMN system for VPC and routing management in ATM networks. In *Integrated Network Management IV* (pp. 356-369). Springer US.

[3] [routed] Periasamy, R., Pandian, G., Bordonaro, F. G., Naderi, R., & Patel, K. A. (2000). *U.S. Patent No. 6,023,733*. Washington, DC: U.S. Patent and Trademark Office.

[4] Clements, M. T. (2004). Direct and indirect network effects: are they equivalent?. *International Journal of Industrial Organization*, *22*(5), 633-645.

[5] Fox, A., Gribble, S. D., Chawathe, Y., Brewer, E. A., & Gauthier, P. (1997, October). Cluster-based scalable network services. In *ACM SIGOPS operating systems review* (Vol. 31, No. 5, pp. 78-91). ACM.

[6] Zou, C. C., Towsley, D., & Gong, W. (2004). A firewall network system for worm defense in enterprise networks. *University of Massachusetts, Amherst, Technical Report TR-04-CSE-01*.

[7] Zhang-Shen, R., & McKeown, N. (2008, April). Designing a fault-tolerant network using valiant load-balancing. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE* (pp. 2360-2368). IEEE