Dustin Mcclure

Jonathan Korstad

Matthew Moklebust

Nekoashi Wolf

CIS 305 Final Project

***1.1 Introduction***

This paper will discuss the implementation of a virtual private cloud within CloudStack. “CloudStack Virtual Private Cloud is a private, isolated part of CloudStack. A VPC can have its own virtual Network topology that resembles a traditional physical Network. You can launch Instances in the virtual Network that can have private addresses in the range of your choice. (Apache CloudStack n.d.) This type of cloud is the typical configuration for users that require the highest level of security within their computing environment. Governments, financial or legal firms, schools and healthcare providers are all users of this type. We will use a combination of existing CloudStack image templates VMs, templates we created per the CloudStack documentation, and the online CloudStack VPC documentation to configure the VPC. This should take around 4-6 hours to complete.

***1.2 Advantages and Disadvantages***

Some advantages of implementing a VPC are greater amount of flexibility, with users being able to “…quickly and easily deploy and manage their resources without having to worry about hardware or physical infrastructure limitations” (Hi Cloud n.d.), and scalability, allowing the growing and shrinking of the resource pool to accommodate the current needs of a VPC user. Security improvement, one of the other advantages of using a virtual private cloud, can also be a disadvantage for certain clients. For many public and private sector entities who choose to use a virtual private cloud, one of the motivating factors in moving from something like a public cloud is improved security with the ability to "... create a private network environment that is isolated from the public internet” and “…define their own security groups and access control policies” (Hi Cloud n.d.), but some companies or public entities that have to follow strict regulations such as PCI-DSS may only be able to place certain apps or data in a VPC, and because of this it may not be worth the investment. (Gomez, J., Insignares, A., Kazmi, R., & Tarud, J. 2023, December 1)

While there are many advantages that come with using a VPC, there are also disadvantages, with the primary disadvantages being cost, complexity, and reliance on third parties (namely your ISP and cloud provider). Setting up and maintaining a VPC can be quite expensive with the possibility of users needing to spend additionally for things like data transfer operations, IP address space allocation, and other costs on top of running their infrastructure (Hi Cloud n.d.) In addition to cost, implementing, configuring, and maintaining a VPC can be complex with the need to manage multiple “…components, such as subnets, routing tables, security groups, and network ACLs…” (Hi Cloud n.d.) Possibly the most readily apparent drawback for many is that you no longer have direct physical access to your equipment and data, instead you must rely on the reliability of your internet service provider and cloud provider; if either if these fail you may lose access to much of your infrastructure.

***1.3 VPC Configuration Process***

This configuration assumes that a host like KVM is already installed on the management server. The first step in the configuration process is to specify an advanced zone. You will need to first choose the infrastructure option from the left-side navigation menu, select zones, and then select “Add Zone +”. At this point the zone creation wizard modal will pop up, you will need to select the core option, and then you will need to select the Advanced option. Do not activate the “Security Groups” radio button as security groups are not supported with VPCs in CloudStack. At this point a window will appear where you can choose the name, external and internal DNS providers, network domain, hypervisor type, guest CIDR range, whether the zone should be dedicated, and whether or not local storage for user interfaces and system VMs should be enabled. The next task is to create one or more Physical Networks that will be associated with the Zone, decide how you would like to isolate traffic on these networks, and then choose the types of traffic that will traverse the Physical Networks; the choices are Management, Guest, Public, and Storage. Network traffic labels can also be defined by clicking on the edit button next to each traffic type. As part of the network creation process, you must also specify at least one range of IP addresses by which VMs in your VPC can implement NAT (network address translation) between their guest network (public/private network or network tier) and their public network (any network outside of these defined networks).

The second step is the configuration of the pod. A menu will come up that will allow you to select a pod name, reserved system gateway, reserved system netmask, and start/end and reserved system IP address. You can push the next button to configure which VLAN or VXLAN range should be used for communication between end-user VMs, and then next again to specify which subnet/VLAN/IP range storage traffic should traverse.

The next item to be configured is the cluster. Here you will choose a cluster name. CloudStack will add primary and secondary storage automatically, but the user will need to specify the host (fqdn or ip) and username/password or ssh keypair to the server where storage resides. A name as well as a protocol will need to be selected. For KVM the correct choice is NFS. This will also need a server and path.

The next step is to login into CloudStack and choose the network option in the navigation bar on the left. After selecting VPC under this menu and then “Add VPC +”, a name, description, zone, CIDR and VPC offering should be defined. After this is complete you will need to add network tiers. These are isolated networks that are set up on different VLANs. They can communicate with each other using a virtual router. To add and configure network tiers go to the VPC page showing your new VPC, select the new VPC by clicking on its name, choose “Networks” from the menu on the left, and then click “+ Add new tier” at the top. A name, network offering, gateway, netmask, VLAN, and ACL can be defined here. Depending on the type of network offering you may or may not have to define some of these options.

Cisco defines NAT as “a service that operates on a router or edge platform to connect private networks to public networks like the internet.” (Cisco n.d.) In CloudStack static NAT will connect a private IP address to the public one allowing the internal virtual machines to connect to the internet. To set up this feature you will need to enter the VPC configuration area. Under the Public IP addresses section select “+ Acquire new IP”, choose your newly acquired IP from the list, and then select the static NAT button (a circle with a + sign in the middle). The last step is to select the tier and instance.

The final stage to set up a virtual private cloud on CloudStack is the implementation of port forwarding rule(s). It is also found under the configuration section of the VPC. The initial step is to select the Public IP addresses, choose public IP address you would like to add a port forwarding rule for, and then configure the port forwarding rule in the port forwarding tab. You will need to add a private port (range), public port (range), and protocol before clicking the “Add” button to choose the tier and instance for the new rule.

There are some other features that could be added to the virtual private network within CloudStack. “An access control list includes which user, device or program has access to a particular resource such as a printer, folder, or file, on a corporate network or computer.” (Andrews et al., 2019) In CloudStack the access control list defines who can access computing resources. It also specifies their level of access. Another aspect of CloudStack that we did not explore was that of load balancing. This feature allocates system resources to different servers to maximize speed and efficiency. Our virtual machines would not be experiencing significant traffic, so this option was not configured. CloudStack has the option of adding a private gateway to further segment the network. This can be set up in the VPC configuration section. We did not implement these options because we were trying to keep the deployment as straightforward as possible.

***1.4 Our Experience***

In our own deployment of CloudStack for this project it was straightforward to get the management server up and running, create our zones, pods, clusters, and configure storage. We had all done this at least once in class, if not multiple times. We counted this part as a success because we were able to successfully get the foundational aspects of the project up and running with little effort or error on our part.

While we were familiar with some of the foundational aspects of CloudStack, it is quite complex in its entirety, and we had not really touched on many of the core topics necessary to create a VPC apart from reading the documentation. When we started the VPC creation process the area that gave us the most trouble was IP addressing and virtual routing. Because these were things that we started configuring with the initial advanced zone creation, if we had done it incorrectly or missed something when we did this, we had to either delete the clusters/pods/instances/zones/physical networks/etc. and start over again, or in some cases where CloudStack Manager seemed to glitch on deletion of these resources, delete and re-install CloudStack Manager entirely. We dealt with these difficulties by using multiple different configurations throughout the setup process and then adding or modifying configuration options until we found out what worked. We did all of this with the help of the CloudStack documentation on various processes, multiple YouTube videos from CloudStack or about CloudStack, and other outside documentation from sources like ShapeBlue and Universities.

Our estimates on time were also not realistic. The total time spent was more in the range of 10-12 hours. Much of this was due to our lack of experience and understanding related to CloudStack specific networking and how it works in conjunction with VPCs.

There are many facets of a VPC that can be beneficial to organizations thinking about moving their computing infrastructure to the cloud. CloudStack can be configured to have many virtual private networks to serve customers who need the highest level of security for their cloud computing resources. This can be accomplished in a relatively short amount of time with basic knowledge of the CloudStack application.

**References**

Apache CloudStack. (n.d.). Configuring a Virtual Private Cloud. Retrieved November 26, 2023, from

https://docs.cloudstack.apache.org/en/latest/adminguide/networking/virtual\_private\_cloud\_co nfig.html

Cisco. (n.d.) What is network access translation? Retrieved November 26, 2023, from

https://www.cisco.com/c/en/us/products/routers/network-address-translation.html

Andrews, J., Dark, J., & West, J. (2019). Guide to operating systems and security (10th ed.) Cengage.

Bond, J. (2015). The enterprise cloud. Best practices for transforming legacy IT. O’reilly.

Advantages and disadvantages of using VPC for your infrastructure. Hi Cloud. (n.d.).

https://www.hicloud.sg/news/blog/what-is-virtual-private-cloud

Gomez, J., Insignares, A., Kazmi, R., & Tarud, J. (2023, December 1). What is virtual private cloud (VPC) computing?. Koombea.

https://www.koombea.com/blog/what-is-virtual-private-cloud/