ISSN 2394-3777 (Print)
ISSN 2394-3785
(Online)
Available online at
www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

Geographical Routing for Azure Virtual Machine

(January 2018)

Miss Hemalatha M.E – Assistant Professor,
M Swatika – UG Scholar,
M Hinduja – UG Scholar,
N Meena – UG Scholar,
Department of Information Technology,
Paavai Engineering College, Namakkal.

Abstract-The websites that are hosted in any cloud servers are meant to be available to the users all the time. Even the downtime for a fraction of second will lead to the loss of quality of service of the site. To make the website available to the users at a rate of 24/7, we are making us of two different concepts namely Load Balancing and Traffic Managing. Also the website is hosted in virtual machines in different regions so that they will be available in different locations in different forms for different users. There will be no downtime for the website since it will be hosted in multiple virtual machines at different data centers.

INTRODUCTION

Microsoft Azure provides multiple services for managing how network traffic is distributed and load balanced. You can use these services individually or combine their methods, depending on your needs, to build the optimal solution .In this tutorial, we first define a customer use case and see how it can be made more robust and performance

1.1 Existing of Load Balancer:

Server load balancing provides scalability and high availability for applications, Web sites and cloud services by monitoring the health of servers, evenly distributing loads across servers and maintaining session persistence and a seamless user experience in the event that one or more servers become overburdened or unresponsive. Load balancing is a application delivery controllers (ADCs) represents application delivery controllers (ADCs) represent a considerable USES Delivers high availability and network performance to your applications. It is a layer S4(TCP UDP) load balancer that distributes incoming traffic among health instances of services.

1.0 Existing of Traffic Manager :

Traffic Manager uses the Domain Name System (DNS) to direct client requests to the most appropriate

endpoint based on a traffic-routing method and the health of the endpoints. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region. USES Improve availability of critical applications Improve responsiveness for high-performance applications. Performance service maintenances without downtime

2.0 Virtual Network :

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network. A virtual network is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or to your on-premises network. The following picture shows some of the capabilities of the Azure Virtual Network service

2.0.1 Connect Virtual Networks

You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other using virtual network peering. The bandwidth and latency of communication between resources in different virtual networks is the same as if the resources

2.1 Virtual Machine:

Service enables azure resource to securely communicate with each other. A "virtual machine" was originally defined by Popes and Goldberg as "an efficient,

ISSN 2394-3777 (Print)
ISSN 2394-3785
(Online)
Available online at
www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

isolated duplicate of a real computer machine."[1]Current use includes virtual machines which have no direct correspondence to any real hardware. The desire to run multiple operating systems was the initial motive for virtual machines, so as to allow time-sharing among several single-tasking operating systems. In some respects, a system virtual machine can be considered a generalization of the concept of virtual memory that historically preceded it. IBM's CP/CMS, the first systems to allow full virtualization, implemented time sharing by providing each user with a single-user operating system, the Conversational Monitor System (CMS). Unlike virtual memory, a system virtual machine entitled the user to write privileged instructions in their code. This approach had certain advantages, such as adding input/output devices not allowed by the standard system.[3]

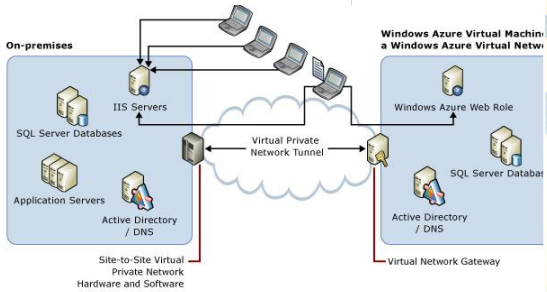

FIG 2.1 VIRTUAL MACHINE

2.2 Load Balancer:

A load balancer acts as the “traffic cop” sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.
In this manner, a load balancer performs the following functions Distributes client requests or network load efficiently across multiple servers

- Ensures high availability and reliability by sending requests only to servers that are online
- Provides the flexibility to add or subtract servers as demand dictates

2.3 Traffic Manager:

Azure Traffic Manager enables you to control the distribution of traffic across your application endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure.

Traffic Manager provides two key benefits:

1. Distribution of traffic according to one of several traffic-routing methods
2. Continuous monitoring of endpoint health and automatic failover when endpoints fail

When a client attempts to connect to a service, it must first resolve the DNS name of the service to an IP address. The client then connects to that IP address to access the service. The most important point to understand is that Traffic Manager works at the DNS level. Traffic Manager uses DNS to direct clients to specific service endpoints based on the rules of the traffic-routing method. Clients connect to the selected endpoint directly. Traffic Manager is not a proxy or a gateway. Traffic Manager does not see the traffic passing between the client and the service

Solution Using These Components

3.0 Architecture:

Load Balancer uses a hash-based distribution algorithm. By default, it uses a 5-tuple hash composed of source IP, source port, destination IP, destination port, and protocol type to map traffic to available servers. It provides stickiness only *within* a transport session. Packets in the same TCP or UDP session will be directed to the same instance behind the load-balanced endpoint. When the client closes and reopens the connection or starts a new session from the same source IP, the source port changes. This may cause the traffic to go to a different endpoint in a different datacenter. Then gives you control over how inbound communication is managed. This communication includes traffic initiated from Internet hosts, virtual machines in other cloud services

ISSN 2394-3777 (Print)
ISSN 2394-3785
(Online)
Available online at
www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

,

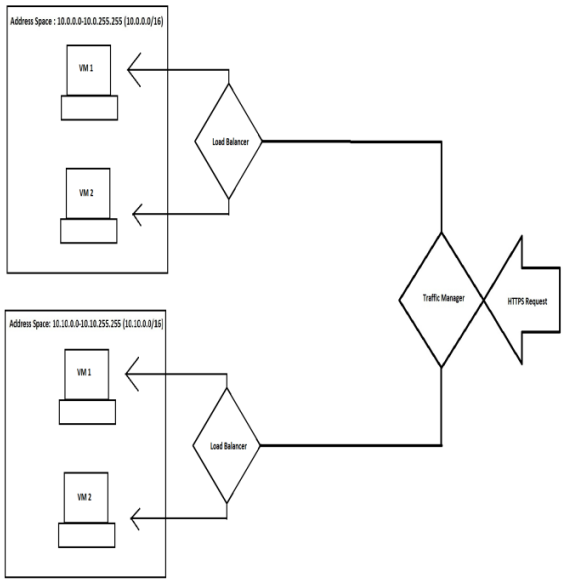

FIG 3.1 LOAD BALANCER

3.2 Architecture : TRAFFIC MANAGER

Priority: Select Priority when you want to use a primary service endpoint for all traffic, and provide backups in case the primary or the backup endpoints are unavailable. Weighted: Select Weighted when you want to distribute traffic across a set of endpoints, either evenly or according to weights, which you define .Performance: Select Performance when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint in terms of the lowest network latency. Geographic: Select Geographic so that users are directed to specific endpoints (Azure, External, or Nested) based on which geographic location their DNS query originates from. This empowers Traffic Manager customers to enable scenarios where knowing a user's geographic region and routing them based on that is important. Examples include complying with data sovereignty mandates, localization of content & user experience and measuring traffic from different regions

.

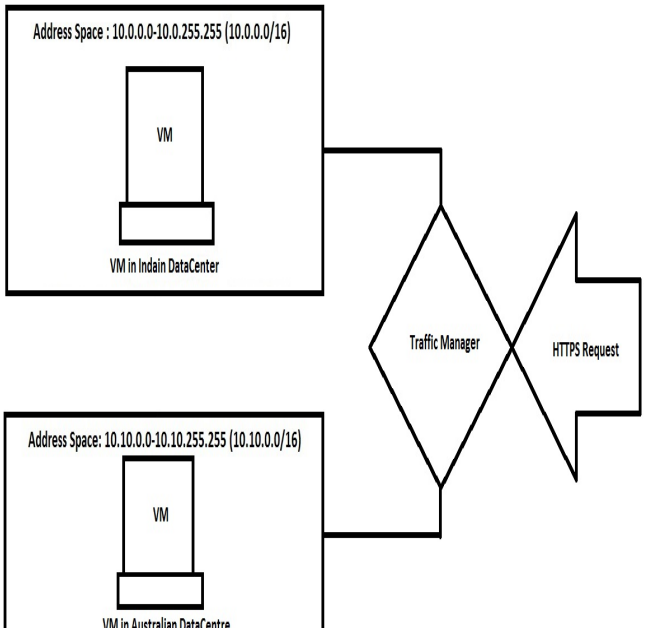

FIG 3.2 TRAFFIC MANAGER

3.2.1 Traffic Manager end point monitoring: Azure Traffic Manager includes built-in endpoint monitoring and automatic endpoint failover. This feature helps you deliver high-availability applications that are resilient to endpoint failure, including Azure region failures.

T

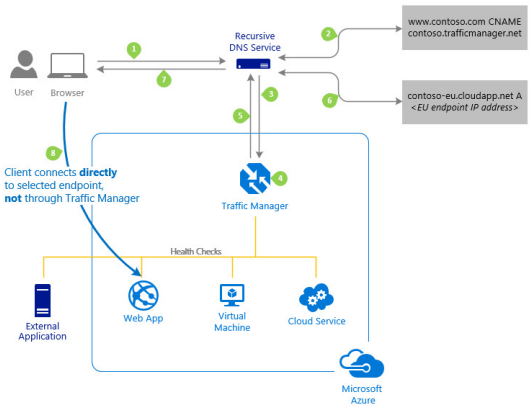

FIG3.2.1 END POINT MONITORING

ISSN 2394-3777 (Print)
ISSN 2394-3785
(Online)
Available online at
www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

3.3ARCHITECTURE OF GEOGRAPHIC ROUTING FOR AZURE VIRTUAL MACHINE

Geographic routing (also called routing or position-based routing) is a routing principle that relies on geographic position information. It is mainly proposed for wireless networks and based on the idea that the source sends a message to the geographic location of the destination instead of using the network address. The idea of using position information for routing was first proposed in the 1980s in the area of packet radio networks [1] and interconnection networks.[2] Geographic routing requires that each node can determine its own location and that the source is aware of the location of the destination. With this information a message can be routed to the destination without knowledge of the network topology or a prior route discovery.

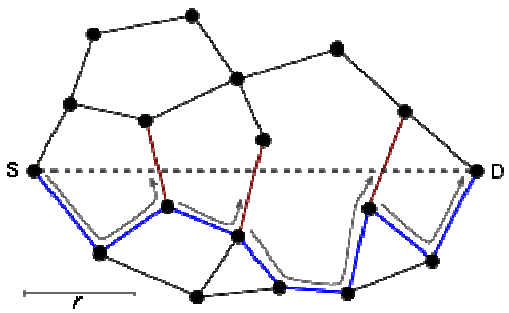

FIG 3.3 GEOGRAPHICAL ROUTING

SCOPE OF THE MODEL

- 4.0 ADVANTAGES: A Virtual Network is created in a data centre in India and two Virtual Machines are hosted over that Virtual Network in a single availability set. Later to this the sample website with some regional data is hosted in the Virtual Machine.
- One more Virtual Network is created in some other region in the world and again a Virtual Machine is created in that Virtual Network and then a website is hosted in it as well. This time the website will be in reference with that specific region.
- Now with the help of these two availability sets, a Load Balancer is configured for those two Virtual Networks so that the incoming request traffic can be routed to a Virtual Machine that is free.
- Now a Traffic Manager profile is configured over those two load balancers with the Geographic Routing so that an appropriate website is shown to the user when they search for the IP address or the DNS of the Traffic Manager.

4.1 TECHNOLOGIES AND COMPONENTS REQUIRED:

Microsoft Azure

Web-Server

Asp.Net

Connect to an on-premises network

- Point-to-site virtual private network (VPN): Established between a virtual network and a single PC in your network. Each PC that wants to establish connectivity with a virtual network must configure its connection independently.
- Site-to-site VPN: Established between your VPN device and an Azure VPN Gateway deployed in a virtual network. This connection type enables any on-premises resource you authorize to access a virtual network. The connection is an IPSec/IKE VPN that provides encrypted communication over the Internet between your on-premises device and the Azure VPN gateway. The latency for a site-to-site connection is unpredictable, since the traffic traverses the Internet.
- Azure Express Route: Established between your network and Azure, through an Express Route partner. This connection is private. Traffic does not traverse the Internet. The latency for an Express Route connection is predictable, since traffic doesn't traverse the Internet.

Filter Network Traffic

- Network security groups**:** A network security group can contain multiple inbound and outbound security rules that enable you to filter traffic by source and destination IP address, port, and protocol. You can apply a network security group to each network interface in a virtual machine. You can also apply a network security group to the subnet a network

ISSN 2394-3777 (Print)
ISSN 2394-3785
(Online)
Available online at
www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

interface, or other Azure resource, is in. To learn more about network security groups, see Network security groups.

- Network virtual appliances: A network virtual appliance is a virtual machine running software that performs a network function, such as a firewall. View a list of available network virtual appliances in the Azure Marketplace. Network virtual appliances are also available that provide WAN optimization and other network traffic functions. Network virtual appliances are typically used with user-defined or BGP routes. You can also use a network virtual appliance to filter traffic between virtual networks.

Route Network Traffic

Azure creates route tables that enable resources connected to any subnet in any virtual network to communicate with each other, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

- User-defined routes: You can create custom route tables with routes that control where traffic is routed to for each subnet. To learn more about user-defined routes, see User-defined routes.
- BGP routes: If you connect your virtual network to your on-premises network using an Azure VPN Gateway or Express Route connection, you can propagate BGP routes to your virtual networks.

CONCLUSION

In todays networked life a working internet infrastructure is an essential element for productive work. This structure only works with complex technologies like the different routing protocols, this paper demonstrates the complexity of such technologies on the IS-IS routing protocol. This protocol is one of the most complex routing protocols but it is also one of the most reliable protocols with which the biggest and most stable network infrastructures are realized With this online wikipedia elaboration we hope to fulfill the missing online documentation which covers the whole spectrum of this great protocol. Take a look at for the complete draft and help to make it to a real work of reference.

REFERENCES

[1] **Microsoft** " Azure Virtual Network " Link - https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

[2] **Microsoft** " Announcing the General Availability of Geographic Routing capability in Azure Traffic Manager" Link - https://azure.microsoft.com/en-in/blog/announcing-the-general-availability-of-geographic-routing-capability-in-azure-traffic-manager/

[3]**Microsoft "** Traffic Manager routing methods" Link- https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods/

[4]**Microsoft "** Configure the geographic traffic routing method using traffic manager"link- https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-configure-geographic-routing-method

[5]**Microsoft "** Country/Region hierarchy used by Azure Traffic Manager for geographic traffic routing method"Link- https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-geographic-regions

[7]**Microsoft "** Traffic Manager Frequently Asked Questions (FAQ)"Link- https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-faqs

[8] **Microsoft "** Configure priority traffic routing method in Traffic Manager"Link-https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-configure-priority-routing

[10]**Microsoft "**Load Balancer Documentation" Link- https://docs.microsoft.com/en-us/azure/load-balancer/

[11] **Microsoft** "Microsoft Azure Documentation" Link- https://docs.microsoft.com/en-us/azure/

[12] **Microsoft "** Microsoft Azure Documentation" Link- https://docs.microsoft.com/en-us/azure/

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

[13] Microsoft "Azure Virtual Network Service Endpoints" Link-
https://blogs.technet.microsoft.com/ripom/2017/09/30/azure-virtual-network-service-endpoints-preview/

[14] Microsoft "Power Shell Core and Jenkins" Link-
https://blogs.technet.microsoft.com/automagically/2018/01/23/powershell-core-and-jenkins/

[15]] Microsoft "Quick Start with Microsoft Azure" Link-

https://docs.memsql.com/quickstarts/v6.0/quick-start

microsoft-azure/

[16]Microsoft "Deploying Azure Virtual machine using Teraform" Link-
https://geekdudes.wordpress.com/2018/01/23/deploying-azure-virtual-machine-using-terraform/

[17]Microsoft "Azure Schedules Maintenance & Downtime For January 9th" Link-http://www.aidanfinn.com/?p=20877