High Availability Solution over Hybrid Cloud Using Failover Clustering Feature

Wagdy A. Aziz

Faculty of Engineering
CHEP: Credit Hours Engineering Programs
Ain Shams University/Orange-Egypt
Cairo, Egypt.
Wagdy.anis@orange.com

Ziad M. ElMehy

Faculty of Engineering
CHEP: Credit Hours Engineering Programs
Ain Shams University
Cairo, Egypt.
ziadelmehy96@gmail.com

***Abstract* - Cloud computing has proposed a new perspective for provisioning large-scale computing resources by using virtualization technology and a pay-as-you-go cost model. However, cloud computing is subject to failures which emphasize the need to address user's availability. Availability refers to the system uptime and the system capability to operate continuously. Providing highly available services in cloud computing is essential for maintaining customer confidence and satisfaction and preventing revenue losses. Different techniques can be implemented to increase the system availability. This paper demonstrates one way of implementing highly available virtualized network element using Microsoft Windows Server and Microsoft System Center tools.**

Keywords - Cloud Computing, High Availability, Failover Clustering, NFV, Private Cloud , Hybrid Cloud , Public Cloud.

I. INTRODUCTION

For meeting ever-changing business requirements, organizations have to invest more in time and budget for scaling up IT infrastructures. However, achieving this aim by own premises and investments not only is not cost-effective but also organizations will not be able to have an optimal resource utilization. Therefore, these challenges have forced companies to seek some new alternative technology solutions. One of these modern technologies is cloud computing, which focuses on increasing computing power to execute millions of instructions per seconds.

Nowadays, cloud computing and its services are at the top of the list of buzzwords in the IT world. It is a recent trend in IT that can be considered as a paradigm shift for providing IT & computing resources through the network. One of the best and most popular definitions of cloud computing is the NIST definition proposed in 2009 and updated in 2011. According to this definition, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Recent advances in cloud computing are pushing virtualization more than ever. In other words, cloud computing services can be considered as a significant step towards realizing the utility computing concept. In such a computing model, services can be accessed by users regardless of where they are hosted or how they are delivered.

The following critical issues are introduced by cloud business models and technologies including load balancing, security, workflow scheduling, data/service availability, and license management.

Availability is a critical factor for cloud computing as it's considered a significant requirement that needs to achieve. The users expect the system to be running 24/7 and thus, different techniques and technologies needed to be applied and implemented. The availability of a system at time 't' is referred to as the probability that the system is up and functional correctly at that instance in time. HA for cloud services is essential for maintaining customer's confidence and preventing revenue losses due to service level agreement (SLA) violation penalties. Cloud providers are promising to provide highly available services and to minimize the system downtime by implementing different solutions and techniques. However, availability is always a questioning matter whether if we can ensure or is it always a subject of failure. Research reports express that about $285 million have been lost yearly due to cloud service failures and offering availability of about 99.91%. In recent years, cloud computing environments have received significant attention from global business and government agencies for supporting critical mission systems.

Cloud computing service outage can seriously impact workloads of enterprise systems and consumer data and applications. Amazon's EC2 outage on April, 2011 is an example of one of the largest cloud disasters. Several days of Amazon cloud services unavailability resulted in data loss of several high-profile sites and serious business issues for hundreds of IT managers. Furthermore, according to the CRN reports, the 10 biggest cloud service failure of 2017, including IBM's cloud infrastructure failure on January 26,

Facebook on February 24, Amazon Web Services on February 28, Microsoft Azure on March 16, Microsoft Office 365 on March 21 and etc., caused production data loss, and prevented customers from accessing their accounts, services, projects and critical data for very long and painful hours. In addition, credibility of cloud providers took a hit in these service failures and unavailability.

This paper is concerned with implementing High Availability solution for a virtualized network element which is Elastix PBX using the Microsoft Windows Server 2012 R2 Failover Cluster Feature.

II. RELATED WORK AND RESEARCH BACKGROUND

A. Related Work:

High Availability refers to the capacity and the ability of a system to provide continuous services. Researchers are mainly concerned about discovering new technologies and different techniques that can improve security, performance, and availability of cloud computing.

Amir et al. presented in [1] a reference roadmap of HA and reliability problem in cloud computing systems for maintaining customer confidence and satisfaction and preventing revenue losses. Throughout [2], Wejdan et al. has discussed different techniques to increase the availability of the cloud performance such as Fault tolerance, Dynamic scalability, load balancing, data replication, clustering VMs, and others. In [3], Varsha et al. showed some surveys on load balancing that describes different algorithms for balancing the workload for the cloud using optimal resources for better efficiency and performance. Vinay et al. in [4] proposes an architecture, based on clustering virtual machines in datacenters for higher availability of resources with improved scalability.

B. Research Background:

Cloud computing is storing, accessing, and managing huge data and software applications over the internet. In this technology the entire data is secured by firewall networks. Cloud computing provides the context of offering virtualized computing resources and services in a shared and scalable environment through the network on a pay-as-you-go model. By rapid adoption of cloud computing, a large proportion of worldwide IT companies and government organizations have adopted cloud services for various purposes including hosting the mission-critical applications and thus critical data. In order to support these mission-critical applications and data, there is need to provide dependable cloud computing environments.

In order to study dependability of cloud computing, the major cloud computing system (CCS) dependability attributes should be identified which can quantify the dependability of cloud in different aspects. Some important attributes for dependable cloud environments have been mentioned previously and include availability.

Five major actors and related roles in cloud environments are described in the NIST Cloud Computing Standards Roadmap document. These five participating actors are cloud provider, cloud consumer, cloud broker, cloud carrier and cloud auditor explained in Table I.

TABLE I. ACTORS IN CLOUD COMPUTING

Actors	Definition
Cloud consumer	Any individual person or organization that has a business relationship with cloud providers and consumes available services
Cloud provider	Any individual entity or organization which is responsible for making services available and providing computing resources to cloud consumers
Cloud broker	An IT entity that provides an entry for managing performance and QoS of cloud computing services. In addition, it helps cloud providers and consumers with management of service negotiations
Cloud auditor	A party that can provide an independent evaluation of cloud services provided by cloud providers in terms of performance, security and privacy impact, information system operations and etc. in the cloud environments
Cloud carrier	An intermediary party that provides access and connectivity to consumers through any access devices such as networks. Cloud carrier transports services from a cloud provider to cloud consumers

NIST specifies that a cloud infrastructure should have the five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. NIST also specifies three primary cloud deployment models: public, private, and hybrid clouds. A hybrid cloud is a composition of two or more distinct cloud infrastructures (private or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. Figure 1 illustrates a hybrid cloud that is composed of an on-premise private cloud deployed by enterprise Q and a public cloud serving enterprise and individual consumers.

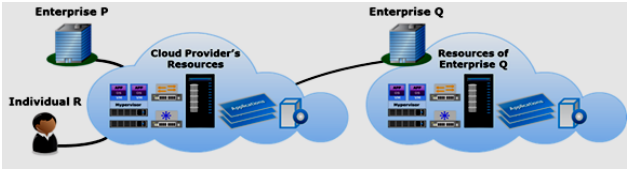

Figure 1. Hybrid Cloud Computing

NIST also specifies three primary cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In the IaaS model, consumers hire IT resources, such as compute systems, storage capacity, and network bandwidth from a cloud service provider. The underlying cloud infrastructure

is deployed and managed by the cloud service provider. Consumers can deploy and configure software, such as operating system (OS), database, and applications on the cloud resources. Typically, the users of IaaS are IT system administrators.

In addition to cloud computing. NFV is an initiative to virtualize network services traditionally run on proprietary, dedicated hardware. With NFV, functions like routing, load balancing and firewalls are packaged as virtual machines. Individual virtual network functions, or Virtual Network Functions (VNF), are an essential component of NFV architecture, as shown in Figure 2. Multiple VNFs can be added to a standard server and then can be monitored and controlled by a hypervisor. A VNF is a logical outcome of NFV. Because NFV architecture virtualize network functions and eliminates specific hardware, network managers can add, move or change network functions at the server level in a simplified provisioning process [5].

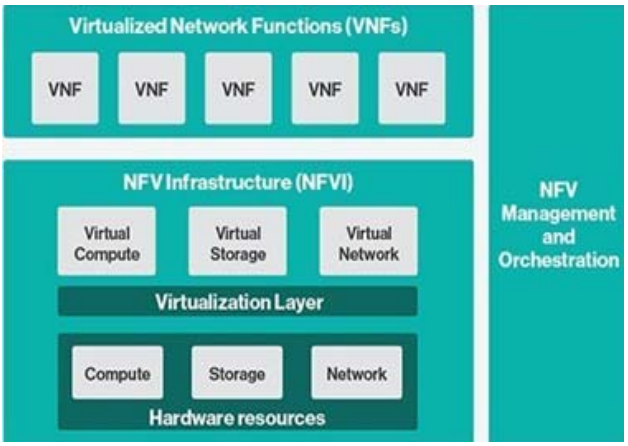

Figure 2. NFV Architecture [5]

III. SOFTWARE ARCHTECTURE TOOLS AND PACKAGAES

A. Cloud PBX [6]

A cloud PBX system is based on Cloud Computing technology, where data is stored and transferred over the Internet, rather than on a computer or piece of hardware that an end-user owns. So, with a cloud PBX provider, you can use all of the standard PBX features without the need of an actual PBX in your home or office. It is a kind of Hosted PBX or virtual PBX, meaning that all of the routing services are performed by a VoIP provider, rather than by an employee managing a PBX system in the office. A cloud PBX works by connecting to your IP, or Internet phone, for its internet connection.

You can access your cloud PBX from any Internet-enabled location or device that you have certified for use with your system. Usually, this is just a matter of logging in with a password or security question from that device. This gives you greater mobility and freedom when using your office phone and PBX.

B. Microsoft System Center 2012 [7]

Microsoft System Center 2012 is Microsoft's solution for cloud and datacenter management as well as client device management and security. System Center 2012 is comprised of a suite of components, each focused on part of the infrastructure management lifecycle. From an IT process automation perspective, the System Center components are the "arms and legs" of the automation capability, which act on end systems while System Center Orchestrator, and the runbooks created within it, are the "brains" of the automation, controlling the order and flow of activities and responding to events during the automated process.

C. Microsoft System Center Virtual Machine Manager [8]

Virtual Machine Manager (VMM) is a management solution for the virtualized data center. You can use it to configure and manage your virtualization host, networking, and storage resources in order to create and deploy virtual machines and services to private clouds that you have created.

Although they have no visibility into the underlying hardware, there is a uniform resource pooling which allows you to add or remove capacity as your environment grows. VMM also supports private clouds across supported hypervisors, such as Hyper-V, Citrix, and VMware.

It has four components which are VMM Management Server, VMM Database, VMM Console, VMM Library and VMM Command Shell.

D. Windows Azure Pack [9]

Windows Azure Pack is Microsoft's on-premise cloud solution that runs on standard server hardware and is ideal for small to midsize businesses. The solution is highly scalable, up to enterprise levels, thanks to the underlying System Center resources. Azure Pack provides a set of Azure technologies for private cloud environments, all provided with Windows Server without additional costs. The solution can also expand and integrate with Azure public cloud components, to create hybrid cloud environments as your business demands.

There are two roles that are used to clarify the use of the two different Azure Pack portals, IT Administrators which refers to the central IT administration team that manages the entire infrastructure and Tenant Administrators which refers to the customer or the self-service portal users. We use the Azure Pack admin portal to manage the environment, tenant capabilities and resources while we use the Azure Pack tenant portal to manage virtual machine environments allocated to them, whether hosted in the data center or at remote sites.

E. Failover Clustering [10]

Failover clusters in Windows Server 2012 provide a high-availability solution for many server roles and applications. By implementing failover clusters, you can maintain application or service availability if one or more computers in the failover cluster fails. If one of the cluster nodes fails, another node begins to provide service. This process is known as failover. A failover clustering solution consists of several components, which include: nodes, network, resource, cluster storage, clients and service or application.

When planning for high availability in a cloud it is important to include Virtual Machines hosting critical applications and services offered in the cloud. The feature named Hyper-V Replica provides asynchronous replication of Virtual Machines from a primary site to a secondary site.

F. Server Message Block [11]

The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Using the SMB protocol, an application (or the user of an application) can access files or other resources at a remote server. Windows Server 2012 introduces the 3.0 version of the SMB protocol that can be used as a sharing protocol for failover cluster.

IV. HIGH AVAILABILITY SOLUTION

The project proposed in our research reported here provides high availability solution for a VNF of a mobile operator, which is a Virtual Machine with cloud PBX-Elastix-installed on it as a proof of concept. Figure 3 shows the topology of the project, which is a hybrid cloud. The on-premises part (private) represents the mobile operator and Microsoft Azure part (public) is the cloud service provider that provides a secondary failover cluster node as a part of a tenant plan. So when the Elastix server fails on premise, the Elastix service (virtual machine) is transferred to the cluster node in Microsoft Azure, making Elastix highly available.

The topology components on-premises are:

AD DS: It is the domain on premises, used for creating and authorizing Service Accounts of Microsoft System Center products. And logged on by all on-premises users and computers.

VMM: The primary virtualization and management product of Microsoft System Center. It is used for adding hosts and clusters to the VMM library and for creating clouds, and so on. An administrator uses VMM for all management tasks including remote ones.

Orchestrator: Its console is installed so that SPF can be installed because SPF is a sub-component of ORCH.

SPF: SPF facilitates communication between Azure Pack and System Center products (VMM in this case). It reflects all changes that the participants (Azure Portals and VMM) made.

Azure Admin Portal: This portal is managed by the on-premises IT administrators and is where user accounts and plans are created, and where resources are assigned to on-premises tenants through linking the users (tenants) with the plans.

Azure Tenant Portal: This portal is used by tenants, the on-premises employees in this case. Tenants can view the services available to them and configure their own environment, such as deploying and managing VMs using the tenant portal.

Failover Cluster Node 1: This is the on-premises node (primary node) of the Failover Cluster which has the virtual machine of Elastix on it along with other VNFs.

The additional components at Microsoft Azure are:

Microsoft System Center: It is a suite of systems management products. The core products are: VMM, ORCH, SM, OM and DPM. They help IT build reliable and manageable systems and better automate processes.

Azure Tenant Portal: This portal is used by azure subscribers; azure subscribers can be individual users or enterprises. In this case the mobile operator is a tenant assigned to a plan created by Microsoft Azure's Admin portal.

Failover Cluster Node 2: The secondary public node of the Failover Cluster which Elastix virtual machine is migrated to and which takes over if node 1of the on premise fails.

SMB: Provides cluster nodes with a shared access to shared storage files.

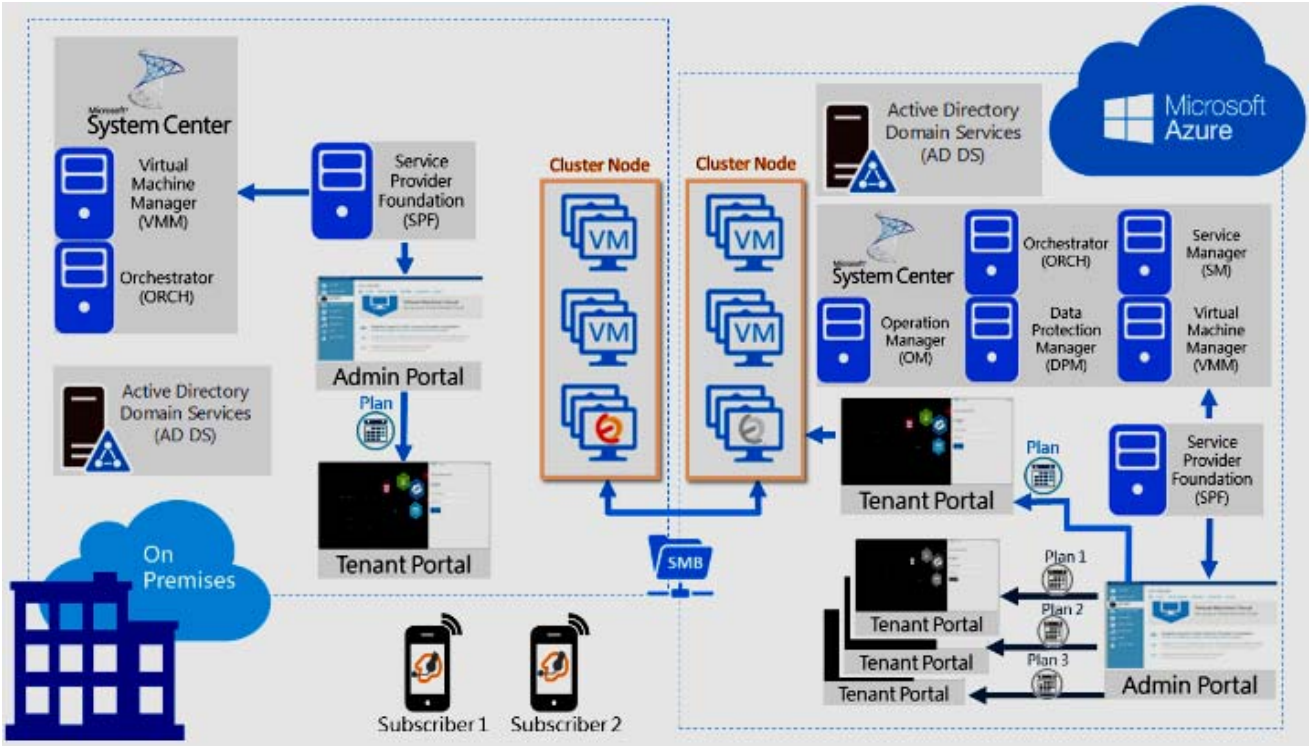

Figure 3. Network Topology of the Project

Zoiper application is installed on the subscribers' mobile phones to make VoIP calls. Using Elastix web portal, a SIP extension is created for each subscriber to be able to create their own accounts on Zoiper.

Initially, a call is initiated between the two subscribers through Zoiper. The two subscribers will access the Elastix server deployed on the on-premises node as demonstrated in Figure 4.

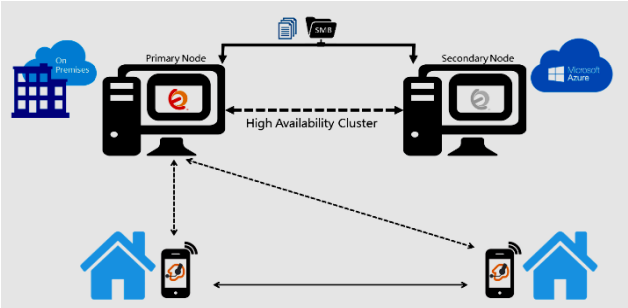

Figure 4. The Call before Primary node failure

In the case of failure of the on-premise node (primary node) while the call is ongoing, the Elastix virtual machine will be migrated to the Microsoft Azure node (secondary node), which now becomes the primary node. The Elastix virtual machine will continue running on the Microsoft Azure node by accessing SMB storage as demonstrated in Figure 5.

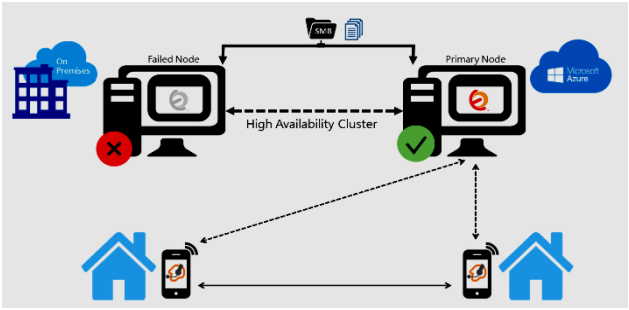

Figure 5. The Call after Primary node failure

During the migration process, the downtime ranges from 2-3 seconds, which is barely recognizable by the user, and then the call proceeds normally. And thus, the voice service using Elastix is proved to be highly available. When the on-premises node is up again, the Elastix virtual machine will be manually migrated using the Failover Cluster Manager.

V. CONCLUSION AND FUTURE WORK

Cloud computing is one of the major revolutions in the world of technology. In order for the user to optimize the benefits that it provides, the availability concerns associated with cloud resources have to be addressed.

The overall goal of this project is providing high availability solution for a virtualized network element using hybrid cloud computing. This will improve the performance

of cloud services, and reduce the downtime of a service, which would otherwise degrade the performance. This paper focused on conducting the solution using Failover cluster feature along with Microsoft System Center tools. Failures that might occur include but are not restricted to the following: network vulnerability, human mistakes, server, storage or power failures and need to be avoided.

As a conclusion, the cloud will remain subject to failure and failures can occur in the cloud as well as the IT traditional environment. Thus, high availability cannot be ensured, but it can be increased and improved, by avoiding common system failures through the implementation of different solutions and techniques. This will be the subject of our future research.

REFERENCES

[1] Mesbahi, Rahmani and Hosseinzadeh, 2018, December. Reliability and high availability in cloud computing environments: a reference roadmap.

[2] Wejdan Bajaber, Manahil AlQulaity, and Fahd S. Alotaibi, 2017, November. Different Techniques to Ensure High Availability in Cloud Computing. In International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 11.

[3] Varsha S. Salunkhe, 2014. Review on Load Balancing Model in Cloud Computing in International Journal of Computer Applications (0975 – 8887).

[4] Chavan, V. and Kaveri, P.R., 2014, August. Clustered virtual machines for higher availability of resources with improved scalability in cloud computing. In Networks & Soft Computing (ICNSC), 2014 First International Conference on (pp. 221-225). IEEE.

[5] Rouse, M (2017). Network Function Virtualization (NFV). [online] Tech Target. Available at: https://searchnetworking.techtarget.com/definition/network-functions-virtualization-NFV [Accessed 18 May 2019].

[6] Voip-info.org, (2019). [online] Available at: https://www.voip-info.org/on-premise-pbx [Accessed 18 May 2019]

[7] Microsoft (2013). Microsoft System Center: Designing Orchestrator Runbooks [pdf].

[8] Microsoft (2014). Technical Documentation for System Center 2012 R2 Virtual Machine Manager [pdf].

[9] Microsoft (2014). CDP-H314 Windows Azure [pdf].

[10] Microsoft (2014). 20412D Configuring Advanced Windows Server® 2012 Services [pdf].

[11] Microsoft.com, 2019. SMB Documentation. [online] Available at: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831795(v=ws.11) [Accessed 18 May 2019].