Network Function Virtualization Over Cloud - Disaster Recovery Solution Over Hybrid Cloud

Wagdy A. Aziz

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

Mina G. Awad

Faculty of Engineering
CHEP: Credit Hours Engineering Programs
Ain Shams University
Cairo, Egypt.
Mina.george.kozman@outlook.com

***Abstract* - In recent years mobile operators have been facing many challenges to achieve the continuity of running services to the users when enterprise datacenter fails. The solution of this project achieves automatically the recovery of datacenter virtual machines by Disaster recovery solution. Disaster recovery (DR) strategy is widely considered as a base-line requirement for many organizations. Historically, DR solutions have been expensive and complex to deploy. This meant that only the largest organizations could afford DR and only then if they had a technically sophisticated IT team. The expense and complexity problems of deploying DR have persisted into recent DR solutions, and this leaves many workloads vulnerable. This then exposes businesses to a range of issues like compliance and audit violations that lead to loss of valuable data. To create a disaster recovery solution, an alternative location must be prepared to be able to recover a datacenter at the occurrence of failure so the business can continue to run. Microsoft Azure is the public cloud to offer Disaster Recovery solutions for applications running on Infrastructure as a Service (IaaS) by replicating VMs into another region even when failure occurs on a region level.**

Keywords - Mobile Operators, Disaster recovery, System center, Microsoft azure

I. INTRODUCTION

A, Cloud Computing

It 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. Cloud computing provides the following services as shown in Figure 1[7].

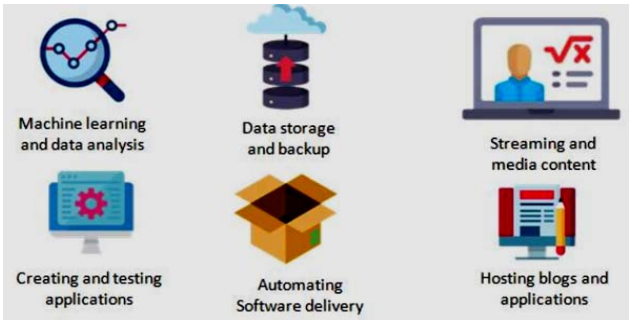

Figure 1. Cloud services [7]

B. Cloud Deployment Model

A cloud infrastructure may be operated in one of the following deployment models: public cloud, private cloud, community Cloud, or hybrid cloud. [7].

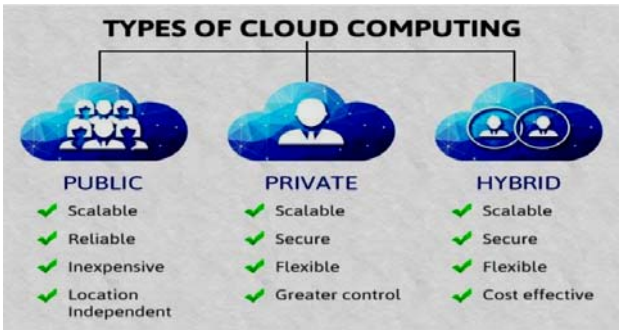

Figure 2. Types of cloud computing [7]

C. Cloud Service Model

C1. Software as a service (SaaS): in which a third-party provider hosts application and makes them available to customers over the internet [7].

C2. Platform as a service (PaaS): in which a third-party provider delivers hardware and software tools, usually those needed for application development to its users as a service [7].

C3. Infrastructure as a service (IaaS): in which a third-party provider offers virtualized computing resources such as VMs and storage over the internet [7].

D. Network Functions Virtualization (NFV)

NFV is a software-based solution that helps the Communication Service Providers (CSPs) to move beyond the traditional, proprietary hardware to achieve greater efficiency and agility while reducing the operational costs. NFV virtualizes network functions on general-purpose, cloud-based infrastructure to provide more agility, flexibility, simplicity, efficiency, and scalability than legacy infrastructure, while also reducing costs and allowing greater innovation.[8]

An NFV environment allows for IT and network convergence by providing a virtualized infrastructure using the standard virtualization technologies that run on standard hardware devices such as switches, routers, and storage to virtualize network functions.[8].

The main advantages of implementing NFV are as follows:

1. Accelerates the time-to-market by allowing quick deployment of new networking services because you do not need to install specialized new hardware to support changing business requirements. NFV allows Communication Service Providers (CSPs) to try and develop services to meet the growing customer demands, thus reducing the risk associated with new services.[8].
2. Delivers agility and flexibility by allowing to quickly scale services to address changing demands and supports innovation by enabling service developers to self-manage their resources and prototype using the same platform that will be used in production.[8].
3. Addresses customer demands in hours or minutes instead of weeks or days, without sacrificing security or performance.[8].
4. Reduces capital expenditures because it uses commodity-off-the-shelf hardware instead of expensive tailor-made equipment.[8].
5. Reduces operational costs by streamlined operations and automation that optimizes day-to-day tasks.[8].

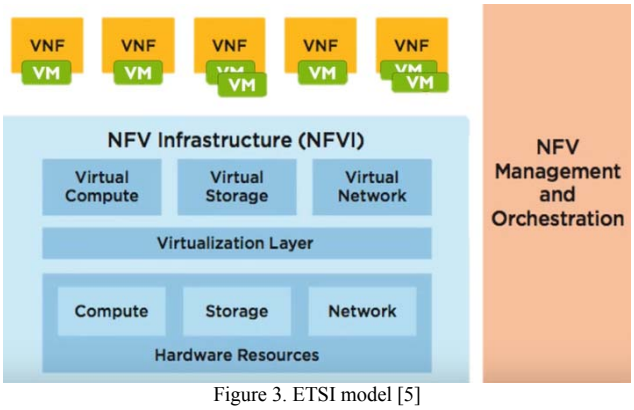

Figure 3. ETSI model [5]

D1. VNF (Virtual Network Function): the software implementation of network functions, such as routers, firewalls, load balancers, broadband gateways and mobile packet processors.[5].

D2. NFV Infrastructure (NFVI): It is the physical resources (compute, storage, network) and the virtualization layer that make up the infrastructure. The network includes the data-path for forwarding packets between virtual machines and across hosts. This allows you to install VNFs without being concerned about the details of the underlying hardware.[5].

*D3. NFV Management and Orchestration (MANO): T*he management and orchestration layer focus on all the service management tasks required throughout the lifecycle of the VNF. The main goals of MANO is to allow service definition, automation, error-correlation, monitoring and lifecycle of the network functions offered by the operator to its customers, decoupled from the physical infrastructure.[5]

II. RELATED WORK

Robert Amatruda Present in [9] a research about Disaster recovery improving time to readiness. J. Antonio Rico, P.E. describe in [10] a Disaster recovery planning which explained the DR vs. Business continuity. Ronald M. Lapedis. Describe in [11] DR plan for Local Area Network (LAN) and disaster recovery plan template for small business continuity. Kruti Sharma, Kavita R Singh describe in [12] the Online Data Back-up and Disaster Recovery and Techniques in Cloud Computing which integrates between site and cloud. In general, these studies aim to provide the continuity of services even through disasters and to prevent data loss. in our work we do not aim only to assure the continuity of service or to protect the whole site from disasters but also to maintain the last updated version of data and to keep the last action of servers saved through DPM server which keeps refreshing the backup stored in it according to the updated actions of site.

Derek Schauland present in [13] his research the Use of Data Protection Manager to ease backups and quickly restore files but in our solution, innovate an automated way using the orchestrator. The automation is the interface between the virtualization and cloud.

III. BACKGROUND

In this section, a description is provided of Microsoft System Center products as a suite of individually sold systems management parts maintaining the Integrity of the Specifications.

A. Virtual Machine Manager (VMM)

VMM is a management solution for the virtualized datacenter, enabling us to configure and manage our virtualization host, networking, and storage resources in order to create and deploy virtual machines and services to private clouds and hosts. VMM is a component of System Center 2012 R2 that discovers, captures and aggregates knowledge of the virtualization infrastructure [2]. VMM architecture consists of several different, interrelated components, which are:

A1. VMM Management Server: The VMM management server is the Virtual Machine or Computer on which the VMM service runs. The VMM management server orchestrates the communication between agents, and supporting resources including libraries, hosts and Virtual Machines, retaining all its configuration and status in the VMM database [2].

A2. Database: The VMM SQL Server database is the primary repository for all configuration and status information. The VMM Service exposes the Database content to the agents, consoles and PS Modules trough an internal communication framework.[2].

A3. Management Console: The management console provides a Graphical User Interface to connect with the VMM management server. The console will initially be the primary method of managing your VMM environment, presenting both virtual and physical infrastructure, offering role-based management access to resources [2].

A4. Library: The building blocks for deploying VMs and Services are stored in the Library. The types of resources hosted in the library include virtual hard disks, and custom resources; both of which are hosted from a library server. Templates, profiles and other resources are hosted directly from the VMM Database. When VMM is deployed in standalone mode the VMM management server will always be the default library server, but you can add additional library servers later. when in clustered mode, a library must be added manually [2].

A5. Command Shell: Windows PowerShell® is the command-line interface into which you use cmdlets that perform all available VMM functions. You can use these VMM–specific cmdlets to manage all the actions in a VMM environment [2].

B. Orchestrator (ORCH)

Microsoft System Center 2016 Orchestrator is the primary IT process automation component of the System Center suite. With Orchestrator, IT pros and/or infrastructure developers can create repeatable automation of repetitive or error prone IT processes in the form of Orchestrator runbooks. Orchestrator runbooks are conceptually similar to scripts in that they perform some set of operations in a repeatable manner. Where they differ is that Orchestrator runbooks can be created by IT pros without as deep of a background in scripting or programming initially but can also include script components in more advanced scenarios. As an IT administrator, you probably perform a lot of tasks and procedures to keep your computing environment healthy. You may have automated individual tasks, but typically, not the whole process. With System Center - Orchestrator you tie disparate tasks and procedures together using a graphical user interface Runbook Designer to create reliable, flexible, and efficient end-to-end solutions in your IT environment.

Orchestrator [6] does the following:

- Automates processes in the data center, regardless of hardware or platform.
- Standardizes best practices to improve operational efficiency [6]
- Connects systems from different vendors without having to know how to use scripting and programming languages [6].

C. Operation Manager (OM)

Is a module in the Microsoft System Center suite of enterprise management software? In simple words, a monitoring tool allows us a look into the health and performance of all our IT services in a single place. It deploys, configures, manages, monitors the services, operations, applications and devices of the various systems within an enterprise and can perform service recovery via a single management console. Simply known as “Operations Manager”, it can monitor the performance of both the clients and server applications. Plus, it can also provide us with info regarding the health of our services across both – cloud and data-center infrastructure. System Center Operations Manager (SCOM), in a single interface, displays all the crucial pieces of your IT environment all at once. This includes security, health, status, performance and configuration. Little components of software called agents can be placed on each device in the company to observe activity. Within the operations manager, we have the power to control the events or alerts chosen to be reported back by the agents. The central System Center Operations Manager server will then store and organize the information [3].

If needed we can even set the notifications to be forwarded to humans to address as necessary. SCOM’s tight integration with other MS servers and applications have made it a popular choice amongst the administrative professionals recently. It is easy to find management packs, i.e. monitoring instructions sets for most current MS operating systems, server applications and third party

software. SCOM or Operations Manager monitors the services and devices and then shares the information regarding them to us as per our requirement.[3].

D. Data Protection Manager (DPM)

System Center Data Protection Manager aims to improve the way Windows admins do backup and recovery with enhanced virtualization capabilities and cloud backup support. System Center Data Protection Manager (DPM) is a robust enterprise backup and recovery system that contributes to your BCDR strategy by facilitating the backup and recovery of enterprise data. You can deploy System Center Data Protection Manager (DPM) for: Application-aware backup: Application-aware back up of Microsoft workloads, including SQL Server, Exchange, and SharePoint. File backup: Back up files, folders and volumes for computers running Windows server and Windows client operating systems System backup: Back up system state or run full, bare-metal backups of physical computers running Windows server or Windows client operating systems. Hyper-V backup: Back up Hyper-V virtual machines (VM) running Windows or Linux. You can back up an entire VM or run application-aware backups of Microsoft workloads on Hyper-V VMs running Windows DPM can store backup data to: Disk: For short-term storage DPM backs up data to disk pools [1].

Azure: For both short-term and long-term storage off-premises, DPM data stored in disk pools can be backed up to the Microsoft Azure cloud using the Azure Backup service Tape: For long-term storage you can back up data to tape, which can then be stored offsite. When outages occur and source data is unavailable, you can use DPM to easily restore data to the original source or to an alternate location. That way, if the original data is unavailable because of planned or unexpected issues, you can easily restore data from an alternate location. DPM uses SQL Server as its database and you protect the DPM server itself for disaster recovery purposes [1].

The method System Center Data Protection Manager (DPM) is used to protect data which varies according to the type of data being protected, and the method of protection selected [4].

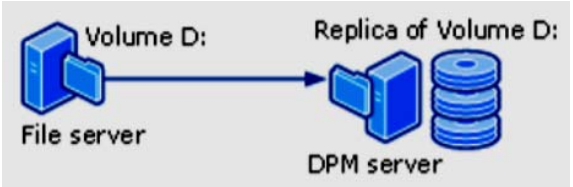

Figure 5. Working Scenario of DPM [1]

Recovery process the method of data protection, disk-based or tape-based, makes no difference to the recovery task. You select the recovery point of data that you want to recover, and DPM recovers the data to the protected computer. DPM can store a maximum of 64 recovery points for each file member of a protection group [4].

Protection policy DPM configures the protection policy for each protection group based on the recovery goals that you specify for that protection group [4].

IV. INTEGRATED FRAMEWORK

A. Differences Between Backups and Disaster Recovery

While having a backup strategy is important, it is not the same as a disaster recovery strategy; rather, the beginning stages of establishing a proper DR plan. A backup is a copy of your data a disaster recovery plan is insurance that guarantees its recovery.

A1. Data Retention Requirements: Backups are typically performed on a daily basis to ensure necessary data retention at a single location, for the single purpose of copying data .Disaster recovery requires the determination of the RTO (recovery time objective) in order to designate the maximum amount of time the business can be without IT systems post-disaster .Traditionally, the ability to meet a given RTO requires at least one duplicate of the IT infrastructure in a secondary location to allow for replication between the production and DR site.

A2. Recovery Ability: Disaster recovery is the process of failing over your primary environment to an alternate environment that is capable of sustaining your business continuity. Backups are useful for immediate access in the event of the need to restore a document but does not facilitate the failover of your total environment should your infrastructure become compromised. They also do not include the physical resources required to bring them online.

A3. Additional Resource Needs: A backup is simply a copy of data intended to be restored to the original source. DR requires a separate production environment where the data can live. All aspects of the current environment should be considered, including physical resources, software, connectivity and security.

A4. Planning Process: Planning a backup routine is relatively simple, since typically the only goals are to meet the RPO (recovery point objective) and data retention requirements. A complete disaster recovery strategy requires additional planning, including determining which systems are considered mission critical, creating a recovery order and communication process, and most importantly, a way to perform a valid test the overall benefits and importance of a DR plan are to mitigate risk and downtime, maintain compliance and avoid outages. Backups serve a simpler purpose. Make sure you know which solution makes sense for your business needs.

B. Our Solution Scenario

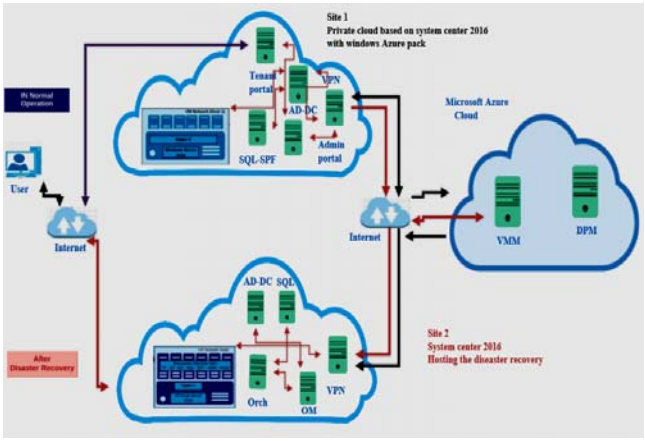

Figure 6. Project Scenario

V. IMPLEMENTATION STEPS

A. DPM Project Implementation Steps

Protection Group and Backup a-Prerequisites:

1) VHD with min. size 60 GB

Select Protection➔New ➔Select Protection group Type

2) Servers for Files and Application Servers

Clients For Data from Laptops and Desktops➔Select Desired Host (Site) and Desired VMS here we select Elastix as it is our Virtual Network Function➔Select Name of Protection group and Method of Protection(Here we select Disk)➔Select Short-term Recovery Goals ➔Select Location of Backup(Which disk)➔Select when to start Backup➔Here we select type of consistency check either if backup is inconsistent from origin or at a specified time.

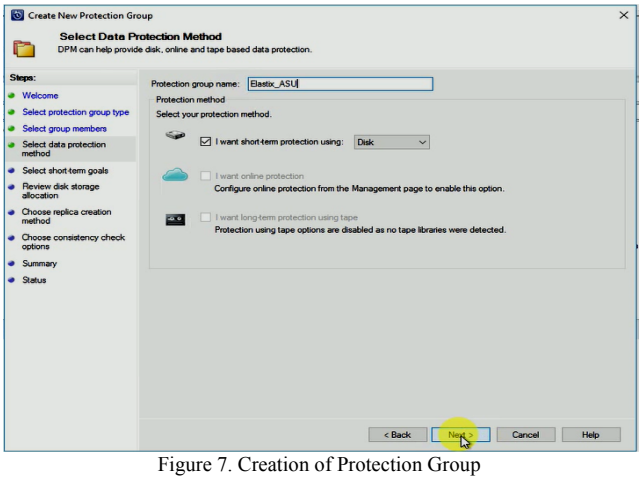

Figure 7. Creation of Protection Group

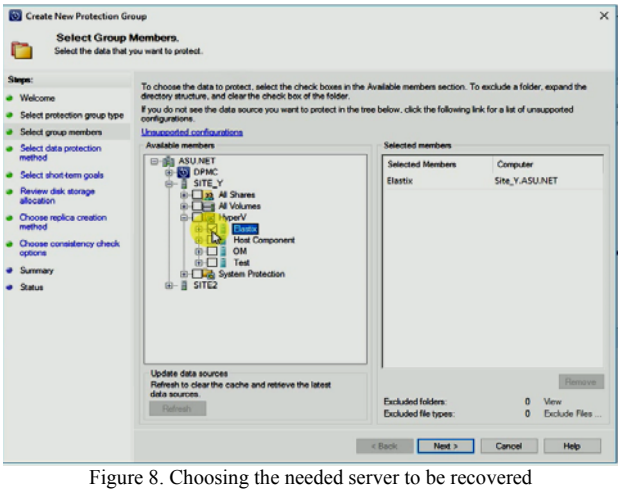

Figure 8. Choosing the needed server to be recovered

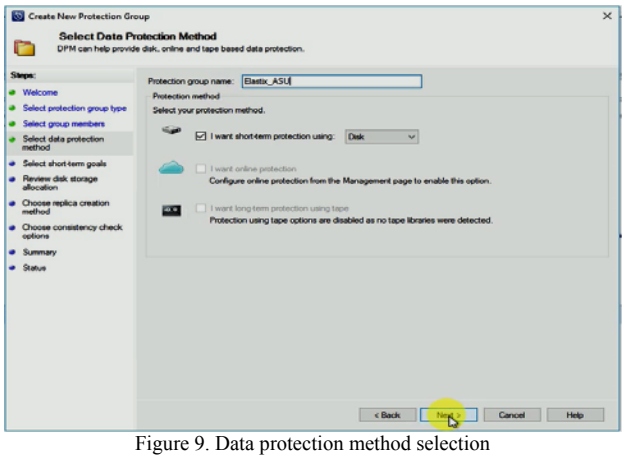

Figure 9. Data protection method selection

B. Orchestrator Project Implementation Steps

Log on to the Orchestrator Server Orchestrator ➔Open the Runbook Designer ➔On the left, under connections, right-click on Runbooks and select New... > Folder➔Give the new folder a name, (Prepare DR - Live Migration)➔On the newly created (Prepare DR – Live Migration) folder, right-click and choose New... > Runbook➔ Rename Runbook (Live Migration) for one time.

- The main function for this Runbook is to decrease the disaster recovery time by make a Live migrate of VMs from Site1.

We try to make this in different ways:

- Using create Template in VMM and deploy it to Host2 in Site2.

The above Runbook has initial values (VM name and Protection group)➔ Threw the Get VM (2)➔ Then shut down the VM to prepare create template form the VM➔We need to take Recovery point for this VM to make sure we

have the last State of VM Therefore, we get Date Source from DPM category We Choose protection group and inter protection group from initialize Data➔Create recovery point➔We get Create Template from VM from VMM category. Enter the script below to make the template and returned value of $template to use it later Note: after this action, we will note that the original VM will destroy as a default action when create the template from VM➔ Then Get VM details➔Then create return the original VM in the original VM➔Get Recovery information➔Recover VM to Original place➔Then start the original VM.

- Using create Move VM in VMM and deploy it to Host2 in Site2

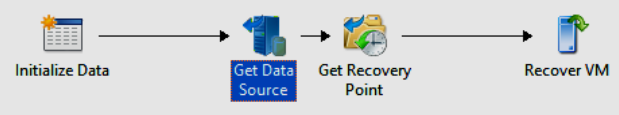

Figure 10. Project Runbook Scenario

The above Runbook has initial values (VM name and Protection group)➔ Threw the Get VM (2)➔We need to take Recovery point for this VM to make sure we have the last State of VM. Therefore, we get Date Source from DPM category. We choose protection group and inter protection group from initialize Date (2)➔ Create recovery point➔Move VM to another host➔Get Recovery information➔ Recover VM to Original place.

- Make an Automated recovery Runbook as shown in Fig. 11 below.

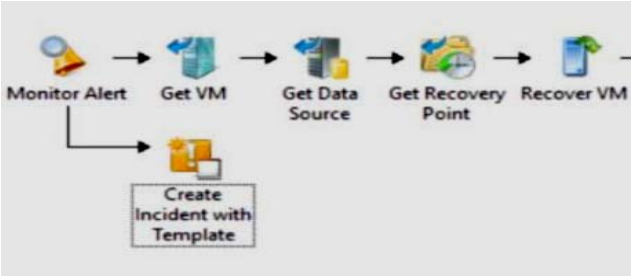

Figure 11. Adding the alert icon on runbook

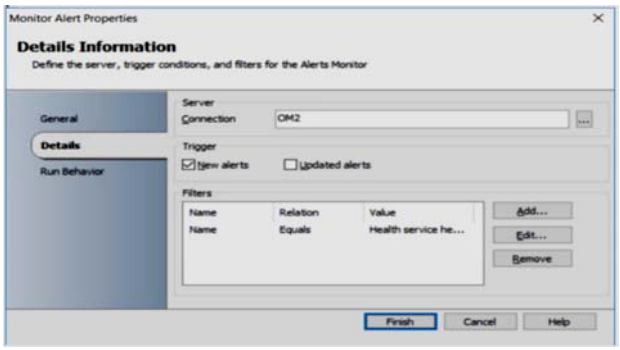

Figure 12. Alert Icon configuration

From Operation manager we get the Alert name➔Create Incident with Template to inform the Service manager that the target VM is down and Orchestrator is take automated action to recovery the target VM➔Get VM details from target VMs➔Get Date Source ID➔Use the Above information to get the last recovery point to recover the VMs to target VM➔Create Incident with Template to inform the Service manager that the recovery process is completed successfully.

C. Operation Manager Project Implementation Steps

Configuring OM for Sending Alert

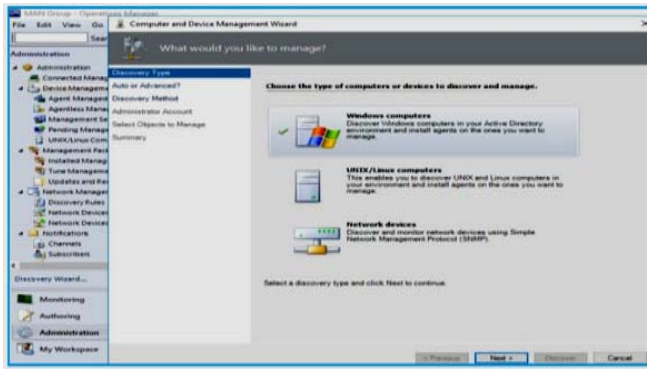

Figure 13. Alert configuration on Operation Manager

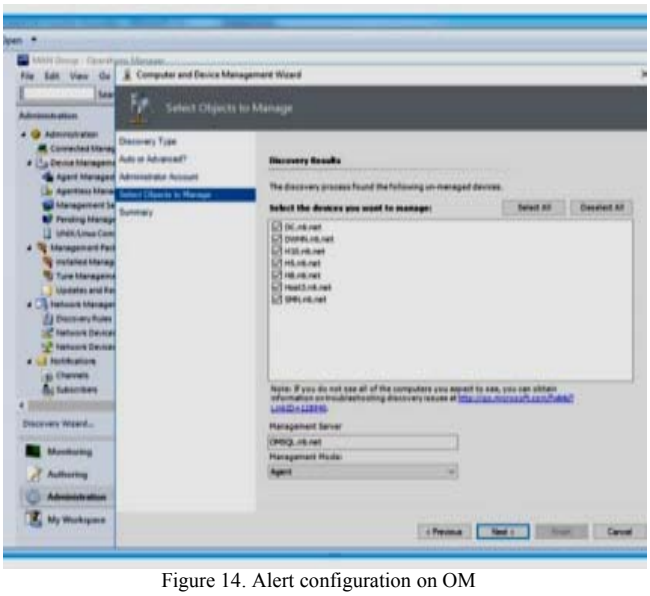

Figure 14. Alert configuration on OM

Create Alert➔rules ➔choose type windows server 2016➔ build event expression ➔choose event id

Alert Appearing

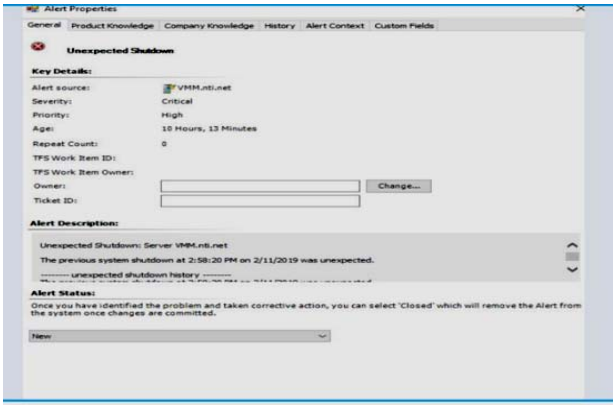

Figure 15. Alert Appearing & status

VI. CONCLUSION

An automated solution ensures that Customer's service is still available (up) and provided even if a disaster has occurred.

This solution is implemented as follows:

- In Normal Situation

Customer can access their service through Microsoft Windows Azure Pack (WAP) portal from site1. System Center Data Protection Manager (DPM) makes a backup for site1 Virtual Machines (VMs). System Center Orchestrator (ORCH) operates a runbook for DPM to take recovery points of (VMs) of site1 to reduce any failure down-time. Then, ORCH operates a runbook for System Center Virtual Machine Manager (VMM) to live migrate virtual machines of site 1. In a scheduled loop, ORCH operates a runbook for DPM to take recovery points of VMs of site1.

- In a Disaster Situation of Site1

System Center Operation Manager (OM) detects failure of site1 and sends failure alert to ORCH. ORCH senses failure alerts, then runbooks is run automatically and operates DPM to perform a recovery for the backed up site1 and add the last recovery points taken. So that a customer can access site2 and find their service up, with decreased down-time.

REFERENCES

[1] (Retrieved from microsoft docs: https://docs.microsoft.com/en-us/system-center/dpm/?view=sc-dpm-2019)
[2] Cardoso, E. A. (2013). Microsoft System Center Virtual Machine Manager 2012 Cookbook . Packt Publishing..
[3] Greene, K. 2016. Getting Started with Microsoft System Center Operations Manager. Packt Publishing - ebooks Account.
[4] Hedblom, Robert. 2015. Microsoft System Center Data Protection Manager 2012 SP1. Packt Publishing.
[5] Howard, M. (n.d.). Retrieved from IEEE ComSoc: http://techblog.comsoc.org/tag/etsi/?fbclid=IwAR3suRwJ9ZKb-NBxh4l-
[6] Steve Beaumont, S. E. (2017). Microsoft System Center 2016 Orchestrator Cookbook (second ed.). Packt Publishing
[7] Avoyan, H. (2017, 10 3). Retrieved from Monitis: https://www.monitis.com/blog/3-types-of-cloud-computing-services/
[8] Retrieved from Redhat: https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/12/html-single/network_functions_virtualization_product_guide/index
[9] Robert.Amatruda https://www.slideshare.net/EMCFORUMINDIA/idc-paper-on-disaster-recovery
[10] Ronald M. Lapedis https://www.slideshare.net/NowAtESEI/esei-drp-white-paper
[11] Kruti Sharma, Kavita R Singh http://chegodaeva.info/disaster-recovery-scenario-template/
[12] Derek Schauland https://www.techrepublic.com/blog/data-center/use-data-protection-manager-to-ease-backups-and-quickly-restore-files/.