

Failover Cluster Assignment

by Yan Zhang

FILE	12042_YAN_ZHANG_FAILOVER_CLUSTER_ASSIGNMENT_181263_12993 8609.DOCX (2.59M)		
TIME SUBMITTED	01-MAY-2019 06:08PM (UTC+0100)	WORD COUNT	3364
SUBMISSION ID	106004890	CHARACTER COUNT	21614



CLUSTER CONCEPTS



Yan Zhang

Table of content

Abstract.....	1
1. Failover cluster construction	1
1.1. Failover cluster.....	1
1.2. Storage Area Network.....	1
1.3. Create virtual machine	2
1.4. Create failover cluster	3
2. Failover cluster concept.....	9
2.1 Work rationale	9
2.2 Correlation between quorum and failover cluster.....	9
2.3 Cluster modes and resource groups	10
2.4 Heartbeat network.....	10
3. Difference between failover cluster and network load balancing cluster.....	11
4. Operation and performance of failover cluster.....	12
5. Deploy software to a failover cluster based on a cloud environment.....	14
6. Other critical concepts	16
Conclusion	17
Reference	18
Bibliography	19

Abstract

This article will introduce the process of setting up a failover cluster, related concepts and working principles. In addition, this article will also compare failover to a network load balancing cluster and discusses deploying software to a failover cluster based on a cloud environment.

1. Failover cluster construction

This chapter will cover the process of building a failover cluster.

1.1. Failover cluster

Failover clustering is a common high availability solution that is implemented by running multiple hardware simultaneously. It must contain three parts: physical server, physical server, storage area network (see figure 1). Traditional hardware or network failure usually requires human participation in troubleshooting, while failover cluster technology does not require human participation and can achieve automatic operation. When a server fails, other servers in the cluster can quickly take over the task and continue to serve users, preventing service failure due to a single server failure. When the failed server comes back online, the cluster service can be set up to allow the original server to failover, thus greatly increasing the ability of the business to continue to be available [1].

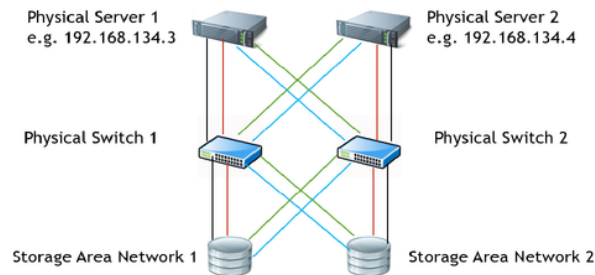


Figure 1 Failover cluster

1.2. Storage Area Network

A storage area network is essentially a set of hard drives. It provides data transfer between computers and storage devices and is an ideal way to meet the basic storage requirements of a high availability cluster. When clusters work, servers often work together to keep applications running, so they need to access the same data [2]. SAN provides the cluster with a storage location for shared data. There are some ways to configure a RAID (see figure 2) [3]:

- RAID 0 - Distributes continuous data across multiple disks for access.
- RAID 1 - Data redundancy is achieved through disk data mirroring, generating.

mutually backed up data on a pair of independent disks.

- RAID 5- Adds parity information based on RAID0.
- RAID 10- Can extract data across disks (like RAID0) and each disk has a mirror disk (like RAID1).

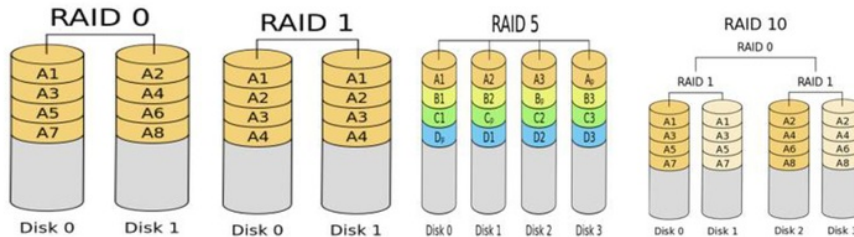


Figure 2 Redundant Array of Independent Disks

In a failover cluster, two areas of storage are required:

- Data – a store of application information and the data is held in a RAID 10 array.
- Quorum – used for cluster management and the quorum is held in a RAID 1 array.

1.3. Create virtual machine

This experiment will set up several virtual machines as the servers in the failover cluster, and these virtual machines were created by the Virtual Machine Manager software (see figure 3).

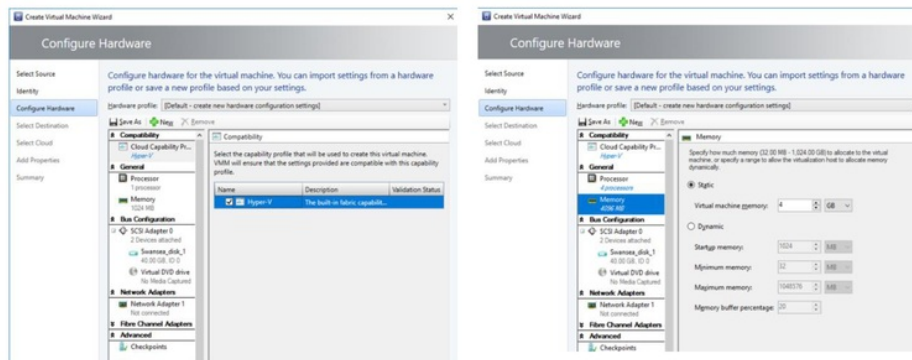


Figure 3 Configuring of virtual machine

Failover clusters are primarily used for Windows operating systems, so the operating system is Windows Server 2016 Standard [4] (see figure 4).

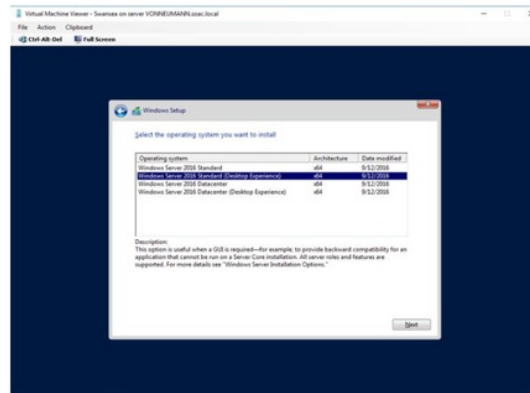


Figure 4 Operating system

After completing the virtual machine installation, the next step is to set up the network and install Servers (see figure 5). Besides, the virtual machine also completed the other configurations, including DNS, DHCP, APR, AD and so on.

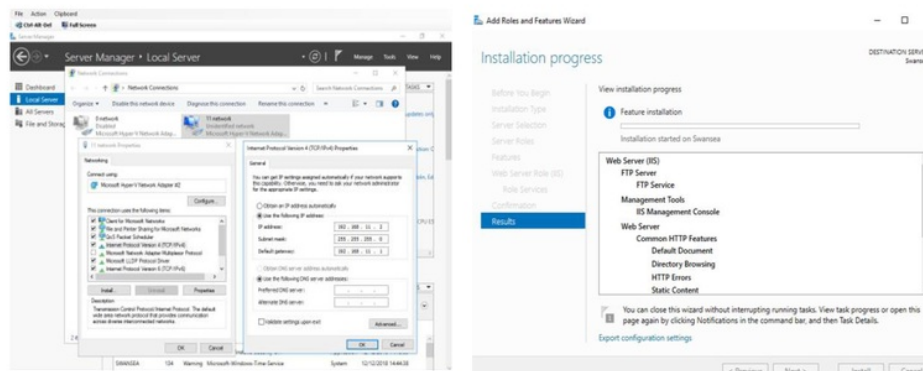


Figure 5 Configuration of network and servers

1.4. Create failover cluster

In this failover cluster setup process, a virtual machine acts as a domain controller with the name cardiff, two virtual machines as nodes, the names are Swansea and Bridgend, and one client machine is named Lab01-01. Among them, the virtual machine named Bridgend will be obtained by cloning the virtual machine named Swansea in the subsequent failover cluster construction process. After completing the above preparatory work, the failover cluster can be set up.

- [1] Step 1: Add a new virtual hard disk to the domain controller and the size is 25GB (see figure 6). Next, divide the disk into two partitions, one of which is 500MB in size and the other partition uses the remaining space on the disk. It is worth noting that the format of both partitions is NTFS.

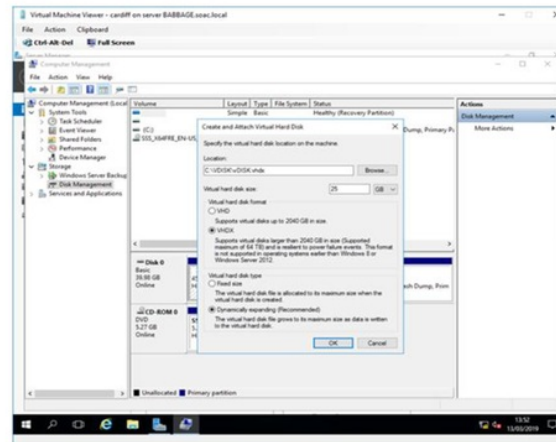


Figure 6 Add a new virtual hard disk

- [2] Step 2: Add the iSCSI target role and create a new iSCSI initiator. This should comprise two dynamically expanding disks [5]. The smaller disks are named "Quorum" and the larger disks are named "Data" (see figure 7).

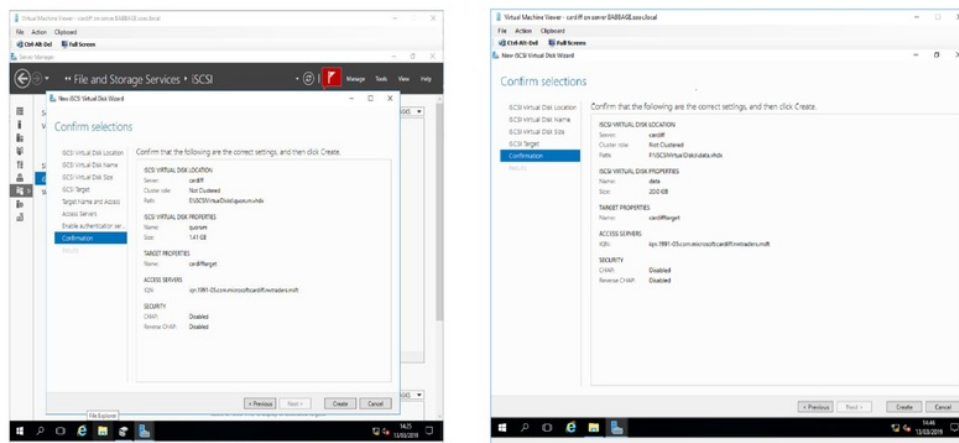


Figure 7 Name the disk

- [3] Step 3: Run the iSCSI Initiator, and both nodes should automatically discover the IP address of the domain controller. Enter 192.168.0.1 in the Target input box, which is the address of the domain controller cardiff and it can auto-discover the targets (see figure 8).

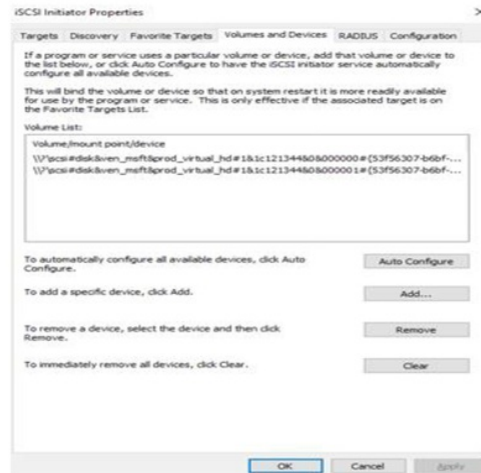


Figure 8 Run the iSCSI Initiator

- [4] Step 4: Bring the disks online but do not allocate them drive. Then add the failover clustering role on both nodes. letters (see figure 9).

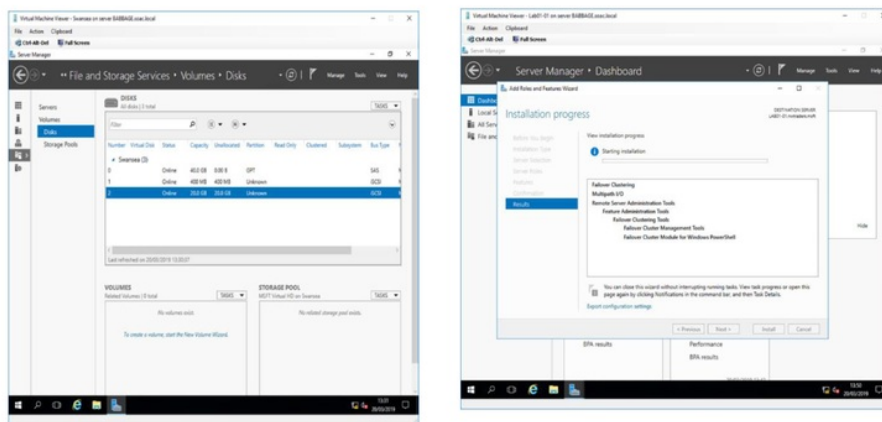


Figure 9 Bring the disks online and add failover cluster

- [5] Step 5: In this step, a virtual machine named Bridgend will be obtained by cloning the virtual machine named Swansea. Now we have four virtual machines, cardiff virtual machine as a domain controller and this new node will work with the

Swansea node as the node of the failover cluster (see figure 10).

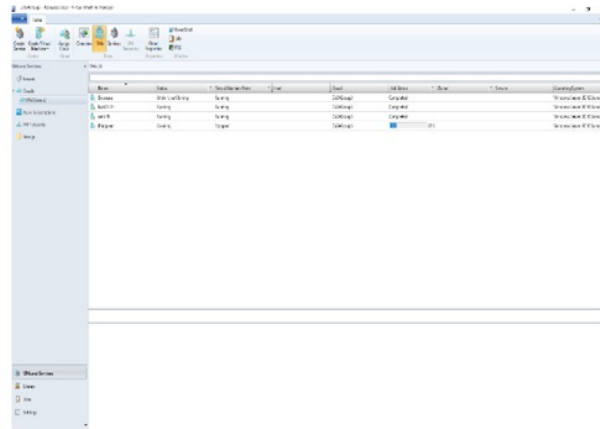


Figure 10 Clone a New Node

- [6] Step 6: It is essential to look at the validate reports and understand the possible warnings. if you understand the warnings, you can continue. If you verify "failed", you must fix the failure before proceeding (see figure 11).

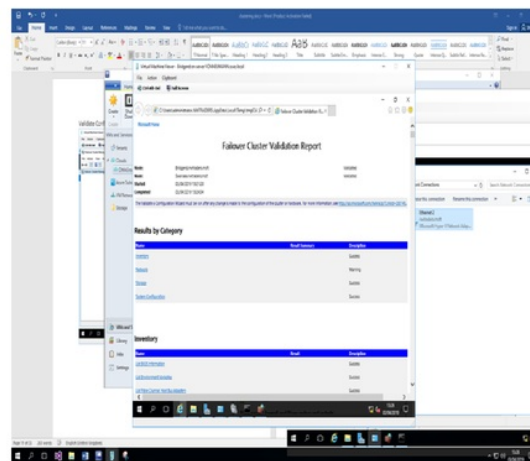


Figure 11 Validate Configuration

- [7] Step 7: Once all failover clusters have been validated, the cluster host can be established (see figure 12). It is worth noting that incorrect firewall settings can cause cluster failures, so shut down the firewall. Besides, network communication between storage and nodes should be secure.

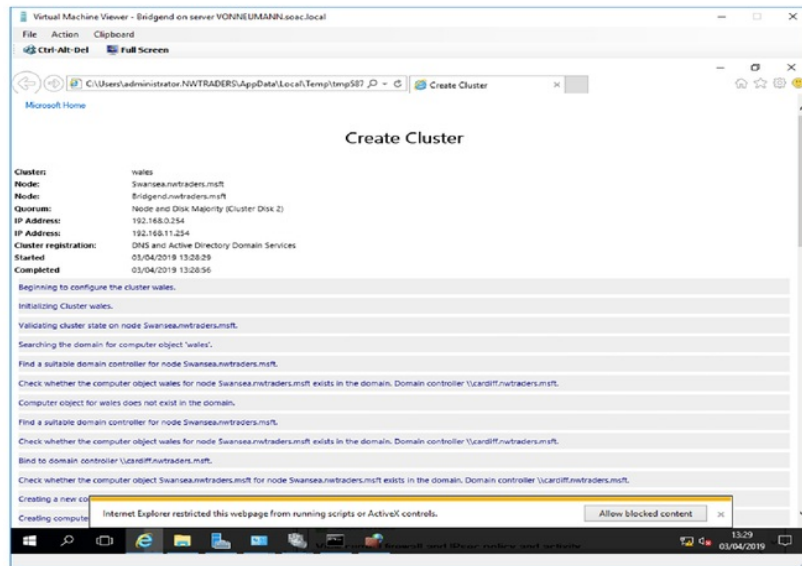


Figure 12 Name the cluster and give it an IP address

- [8] Step 8: Delete the DHCP role from the domain controller and install the DHCP role on both worker nodes (Swansea and Bridgend). Finally, we get the DHCP Server creation report (see figure 13).

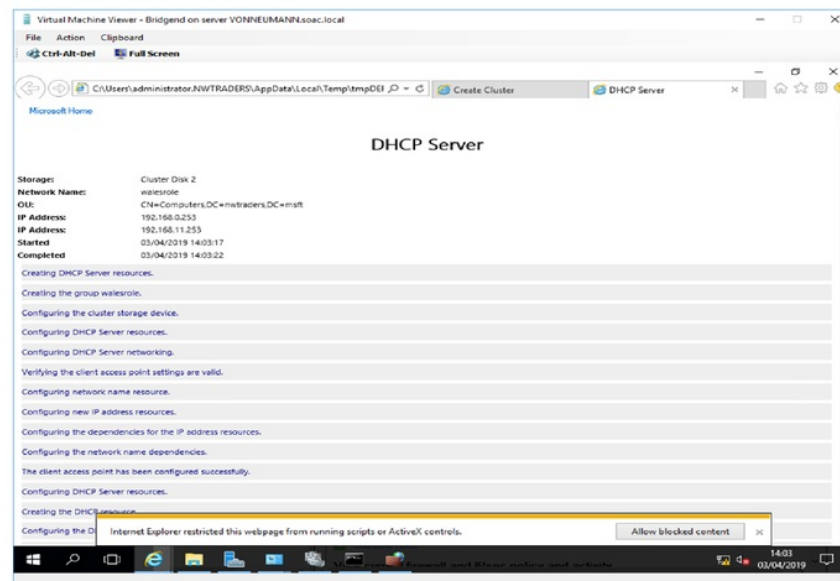


Figure 13 DHCP Server creation report

- [9] After completing the DHCP Server settings, the DHCP Server has started running (see figure 14), and its owner is Bridgend. There are two nodes in this DHCP Server, Swansea and Bridgend. This indicates that the failure cluster has been successfully installed. In this way, when a server in the cluster fails, other servers can take over their work, thus ensuring the normal operation of the application.

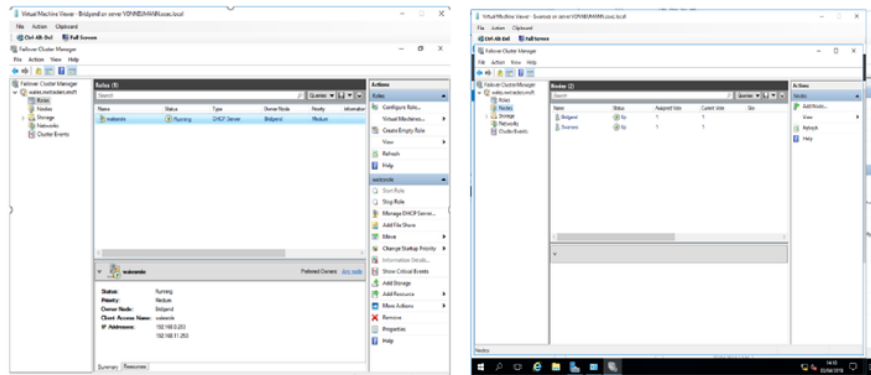


Figure 14 DHCP Server

2. Failover cluster concept

This chapter will discuss the concepts involved in failover clustering.

2.1 Work rationale

Generally, clusters are divided into three basic types according to the tasks to be completed: High-availability Cluster (HA Cluster), High-Performance Cluster (HP Cluster), Load balancing Cluster (LB Cluster) [6].

Failover clustering is one of the high-availability performance clusters designed for applications with long-running in-memory states or large, frequently updated data states [7]. A failover cluster is a domain-based administrative mode deployment that uses a "heartbeat mechanism" to monitor the health of individual nodes. It requires two to eight servers, two or more switches to connect to other components, and two SAN trays (one for data storage and one for the quorum). If the transport host is active, the process is suspended, and the final snapshot of the get process state information is written to the storage device. The receiving host then reads the status information from the shared storage device and resumes the process from the status information. Finally, failover cluster updates the ARP table to update the routing table and redirects the request to the new running node of the process. Therefore, if one server fails, the other servers will take over immediately to keep the application running. Failover may be triggered because:

- A cluster administrator requested it.
- The physical server running that process has become overloaded.
- The server hardware or software running the process has failed, causing the process to fail.

2.2 Correlation between quorum and failover cluster

Quorum, which determines whether the cluster is failover or offline. Typically, the quorum devices in a failover cluster are provided by the SAN [8]. The quorum configuration uses the majority principle. If the number of nodes that are functioning properly meets the number specified by the quorum, the cluster will perform a failover. Otherwise, the cluster will stop working. During the period of service suspension, the normal nodes continuously monitor whether the failed nodes return to normal. When the number of normal nodes returns to the number specified by the quorum, the cluster will work normally.

The majority principle of quorum mode means that all nodes vote. If the proportion of "yes" is more than 50%, the failover cluster will consider that the cluster is in a healthy state, performs failover and continues to provide services. Otherwise, the failover cluster will consider that the cluster has a severe failure, and it will take the cluster offline and stops providing services [9]. According to the composition type of the arbitration node set, the arbitration mode can be divided into the following four types:

- Node majority: Each node has one vote. Allow up to half of the nodes to fail.
- Node and disk majority: Each disk witness and node have one vote. Allow up to half of the nodes to fail if disk witness is online.
- Node and file share majority: Use file sharing like most disks.
- No majority, disk only: Only disks have voting rights.

2.3 Cluster modes and resource groups

A failover cluster mainly include three modes [10]:

- [1] Single-node clustering: single-node clustering is not used for failover and is generally used for simpler shared resources and network storage management. The main advantage is that applications and dependencies are monitored and automatically restarted in the event of a failure or shutdown.
- [2] Multi-node clustering: generally, multi-node clustering is used more frequently. The multi-node clustering mode includes "active, active" and "active, inactive" modes. In "active, inactive" mode, one or more servers are active and can handle client requests, while others are idle. In the "active, active" mode, all nodes are active and can process client requests. If one of the active nodes fails, other nodes will take over the work of this node until it returns to normal.
- [3] More than half a node cluster: in this type, a node may not need to connect to a Shared storage device, and each node may have its storage device. The cluster configuration data can be stored on multiple disks within the cluster so that each node can have its quorum device. Therefore, a more than half node cluster configuration is typically used for servers scattered in different locations.

Resource groups are the basis for cluster failover, such as SAN, iSCSI. Resources that are related or dependent on each other can be considered as resource groups, and all resources that are in the same group must also be on the same node. If one of the services fails, all the services can fail.

2.4 Heartbeat network

The heartbeat network mutually detects the servers in the failover cluster. When the heartbeat signal of the failed server cannot be detected by other servers, the server will be deemed to have failed, and other servers will immediately take over and continue running [11].

The operation is to have all nodes send a "heartbeat" to other nodes - a small packet that says "I am still alive". Do it every 1.2 seconds and if five consecutive heartbeats fail to be detected, the node will failover

3. Difference between failover cluster and network load balancing cluster

Failover clustering is designed for reliability and redundancy. It is designed for software with frequently updated data states and long running memory states. These applications called state applications, typically have data storage capabilities that the server processes based on the information provided by each request and the information stored in previous requests.

Network load balancing [12] is designed to be scalable and reliable, but it has significant limitations on the applications available. Such as FTP servers, proxy servers, and front-end WEB servers are called stateless applications. Typically, the server processes the request based only on the information provided by each request, rather than relying on the information previously requested, so no state data is stored on the server. Because the application is stateless, it does not matter which node receives each request. It does this by communicating with the "virtual" IP that all nodes share. When the NLB cluster receives a request, the request is forwarded to all nodes in the cluster. The host then checks to see if they can service the request and some metadata related to the node with the most recent busy/service request [13]. The relevant nodes request services, respond to clients and modify the cluster metadata based on the selected algorithm.

4. Operation and performance of failover cluster

To ensure that the operation of the failover cluster function, some failure testing can be performed. For the best results, we will turn off one virtual machine. We can see that the DHCP server is running regularly, and its owner is Swansea, and both Swansea and Bridgend nodes are running regularly (see figure 15).

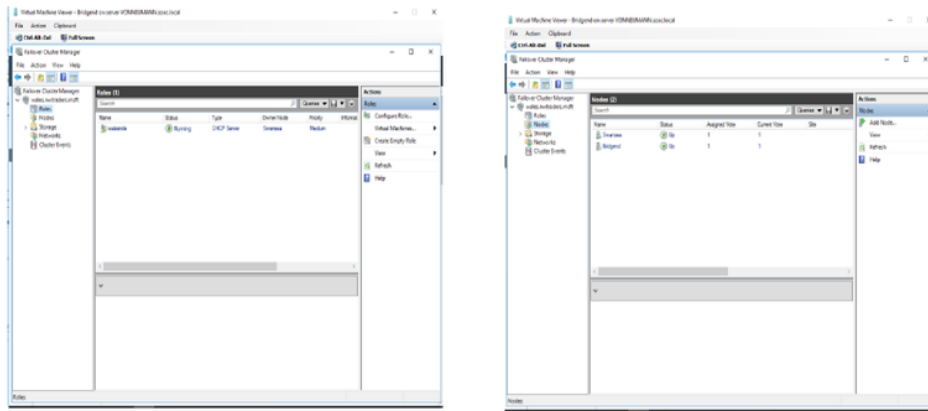


Figure 15 DHCP server on Swansea

After power off the Swansea virtual machine, the failover cluster found the lost Swansea server in less than 10 seconds. At this point, through the quorum ("disk witness"), Bridgend was re-elected as the owner of the DHCP server, and only Bridgend node was left (see figure 16). Finally, the virtual machine was restored to normal, and the experiment was successful.

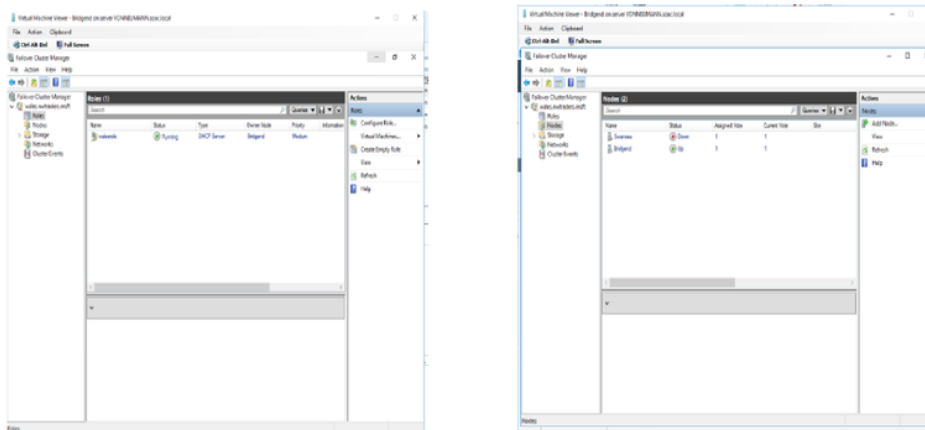


Figure 16 DHCP server on Bridgend

When the Swansea node is restarted, it can rejoin the cluster (see figure 17).

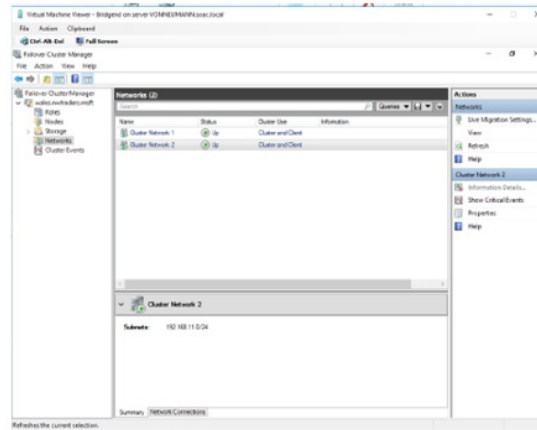


Figure 17 Rejoin the cluster

Figure 18 shows the log of the failover cluster. As can be seen, the log recorded that the Swansea node has been removed from the cluster and has lost contact with the cluster. Therefore, this failover cluster can react quickly when the cluster fails and has proper operation and performance.

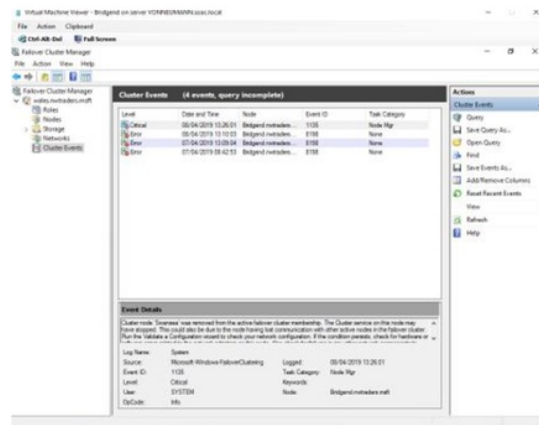


Figure 18 Log of the failover cluster

5. Deploy software to a failover cluster based on a cloud environment

Traditional applications are getting more complex: they need to support more users, they need more computing power, they need more stability and security, and so on. To address these issues, many companies are deploying their applications to the cloud [14]. On the cloud platform, these issues will be addressed by a professional team of cloud service providers and this means using cloud services like a tool. Besides, the failover cluster in the cloud environment will also serve as a whole, providing users with storage space, CPU, and so on, and external machines can be connected to the cluster to deploy software to the cloud environment (see figure 19).



Figure 19 Cloud platform

Take the Google cloud as an example. The Google cloud platform provides high availability failover for many applications. These services work by copying data from the master instance to replica instances in different regions. In order to prevent localized disasters, these replicas are placed in different data centers. If the primary instance of the application fails, the high availability rules failover to the replica instance.

Cloud computing can be divided into three broad categories: private cloud, public cloud, and hybrid cloud. A private cloud is a virtualized data center that meets only one customer's cloud computing needs. This experiment built the failover cluster in a private cloud environment (see figure 20).

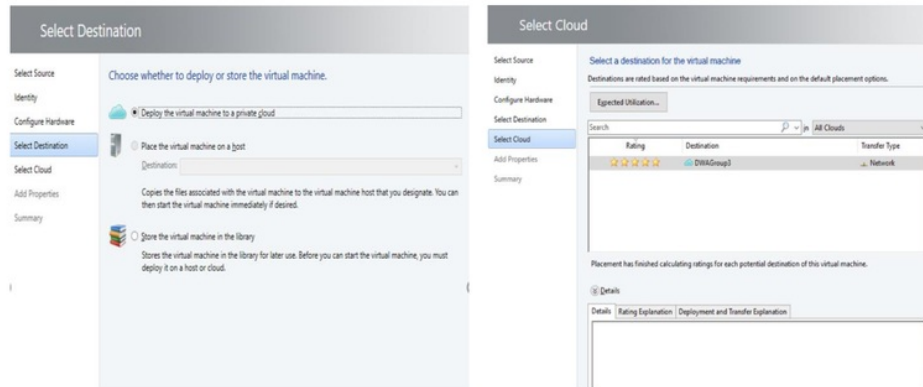


Figure 20 Failover cluster based on a cloud environment

In general, deploying software to a failover cluster based on a cloud environment has the following service advantages:

- Adapt planned downtime maintenance. Failover clustering enables downtime maintenance of a subset of servers in the cluster within a set time frame while maintaining business continuity. With failover clustering, you can do some maintenance during the day without having to work late at night to do it.
- Reduce unplanned downtime. Failover clusters automatically take over services on unplanned downtime servers through their algorithm-based mechanisms, reducing downtime due to hardware or software failures and the impact on business continuity.

In a word, deploying software to a cloud-based failover cluster can not only improve the performance of the software, but also reduce the service failure caused by a server failure, thus maintaining the high availability of the whole system.

6. Other critical concepts

- [1] Clustering: It can be thought of as an extension of parallelism – taking a task, or range of tasks, and running them on multiple physical machines simultaneously.
- [2] Cluster quorum resource: The quorum resource is mainly used to maintain the recovery log, and all changes added by the cluster are written to the recovery log to ensure that the configuration and status of the cluster are restored.
- [3] iSCSI: Small Computer Systems Interface (SCSI) which chained hard drives together in serial.
- [4] Distributed storage: Create two virtual disks using iSCSI, one disk as the quorum disk and the other disk as the shared storage disk.
- [5] DNS: Domain name system is one approach of naming computers, and translating between these names and IP addresses.
- [6] DHCP: Dynamic Host Configuration Protocol. The DHCP server automatically provides client computers and other TCP/ Ip-based network devices with valid IP addresses.
- [7] AD: Active Directory refers to the Directory service in Windows 2000 network, which not only provides a series of Directory service functions for centralized organization and management and access to network resources but also centrally manages access to network resources and allows users to access all resources in Active Directory only once
- [8] ARP: Address Resolution Protocol is used to convert an IP address into the MAC address required.

Conclusion

Failover cluster plays an important role in the actual working environment, so mastering the deployment scheme and principle of failover cluster will not only help enterprises to achieve good economic benefits, but also reduce the work of software developers. In addition, cloud computing is a future development trend, and deploying software to a cloud-based failover cluster will greatly improve software reliability and availability.

Reference

- [1] M. Rouse, "Definition of failover cluster," TechTarget, 7 2012. [Online]. Available: <https://searchwindowsserver.techtarget.com/definition/failover-cluster>. [Accessed 7 4 2019].
- [2] E. Ottem, "Storage Area Networks: Providing High-Availability Storage for Cluster Environments," DELL, 3 2002. [Online]. Available: https://www.dell.com/content/topics/global.aspx/power/en/ps1q02_gadzoox?c=us&l=en&cs=04. [Accessed 7 4 2019].
- [3] M. Rouse, "RAID (redundant array of independent disks)," TechTarget, 5 2017. [Online]. Available: <https://searchstorage.techtarget.com/definition/RAID>. [Accessed 7 4 2019].
- [4] M. Awad, "Setup RD Licensing Role on Windows Server 2012 R2," 6 3 2017. [Online]. Available: <https://social.technet.microsoft.com/wiki/contents/articles/37408.setup-rd-licensing-role-on-windows-server-2012-r2.aspx>. [Accessed 8 4 2019].
- [5] M. D. Francis, "Step-By-Step: Migrating DHCP From Windows Server 2003 to 2012 R2," 25 11 2014. [Online]. Available: <https://blogs.technet.microsoft.com/canitpro/2014/11/25/step-by-step-migrating-dhcp-from-windows-server-2003-to-2012-r2/>. [Accessed 8 4 2019].
- [6] I. D. D. Craig, in *Virtual Machines*, London, Springer, 2006.
- [7] V. M. B. W. S. M. D. B. Brian Svidergol, in *Mastering Windows Server 2016*, Indianapolis, Sybex, 2018.
- [8] B. Posey, in *Hyper-V for VMware Administrators*, Springer Nature, 2015.
- [9] Microsoft, "Windows Server Failover Clustering," Sombers Associates, 2010.
- [10] "Fail Safe Concepts and Administration Guide," ORACLE, [Online]. Available: https://docs.oracle.com/cd/E27731_01/doc.41/e24699/concepts.htm#OFSCN124. [Accessed 10 4 2019].
- [11] Fortinet, "HA heartbeat and communication between cluster units," [Online]. Available: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverHeartbeat.htm. [Accessed 10 4 2019].
- [12] M. W. M. S. R. A B M Moniruzzaman, "A High Availability Clusters Model Combined with Load Balancing and Shared Storage Technologies for Web Servers," 12 2014.
- [13] S. P. R. Godha, "Load Balancing in a Network," *International Journal of Scientific and Research*, 2014.
- [14] A. W. Finn, H. Vredevoort, P. Lownds and D. Flynn, Microsoft private cloud computing, Indianapolis, Ind. : Wiley Pub, 2012.

Bibliography

- [1] Microsoft, " Create a failover cluster" DELL, 3 2002. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster>. [Accessed 7 4 2019].
- [2] Kathryn Pyne Parsons. Three Concepts of Clusters. Philosophy and Phenomenological Research: IEEE. pp. 514–523,1973.
- [3] Chris Amaris, Omar Droubi, Ross Mistry, Rand Morimoto, Michael Noel, in Windows Server 2008 Technology Primer, Pearson, 2008.

Failover Cluster Assignment

GRADEMARK REPORT

FINAL GRADE

62/100

GENERAL COMMENTS

Instructor

Engagement with Literature Skills (50): 29

Knowledge and Understanding Skills (10): 6

Cognitive and Intellectual Skills (15): 9

Practical Application Skills (15): 12

Transferable Skills for Life and

Professional Practice (10): 6

A generally good, well-written report. Good practical work. References could be stronger - some of my diagrams are also uncited.

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21
