Design Template

August Crissy Games

Proof-of-Concept Design Template

Datacenter Virtualization

Ryan Peterson ID 000980429

1-3-2022

[Version 2.0]

WESTERN GOVERNORS UNIVERSITY

CONTENTS

A. SYSTEMS ANALYSIS OF CURRENT ENVIRONMENT

Because of the increasing popularity of role-playing games, such as the latest releases from Augusta Crissy Detective Games, and the growing interest in virtual reality as a gaming technology, current trends indicate that the datacenter should migrate to a more virtual environment. Various factors contribute to this, including the fact that their current datacenter is limited in terms of both space and power rating, among others. With virtualization in a hybrid-cloud datacenter solution, the organization can expand its server space and capacity on top of its existing physical infrastructure.

In order to respond quickly to demand, a hybrid cloud solution would eliminate the need for costly real estate investment or leasing, and the cost of purchasing new hardware would be negligible compared to the costs of purchasing server hardware and datacenter floor space. Virtualization makes it possible to lease server space and then expand it when demand increases. Also, additional virtual servers can be added to the domain in hours rather than days or weeks when waiting for hardware and then developing the system before it is ready to be put into service.

The true goal of developing a virtualized infrastructure is to help Augusta Crissy Games operate in a more lean and agile fashion. With the shared responsibility model of cloud providers, the company can focus on what they do best: developing games. The enormous elasticity and scalability of cloud providers will help the company convert much of its current capital expenditures into operating expenditures, which is more in line with the modern gaming world full of subscription models and in-game purchases. When contrasted to the old world of a singly purchased game developed in a waterfall cycle, this push for virtualization will enable a move towards continuous delivery and improvement, and ultimately a more robust bottom line.

B. VIRTUALIZATION SOLUTION

Following the specifications mentioned in the Overview and Standards of the Company document, a virtualization solution will be installed on an ESXi host in strict agreement with those requirements. A great deal of attention was paid to each individual criterion in order to ensure that the supplied solution not only answered the demand, but also met all of the requirements as well.

HOW THE SOLUTION MEETS THE BUSINESS NEEDS

This proof-of-concept demonstrates some of the benefits of datacenter virtualization technology in order to demonstrate the benefits of virtualization technology in general. The usage of a vSphere Datacenter in conjunction with this solution is recommended, as it will enable for complete active directory integration as well as a greater range of functionality than are available in the free ESXi version of the solution.

HOW THE SOLUTION MEETS THE TECHNICAL REQUIREMENTS

When the proof of concept was deployed, it followed the parameters outlined in the requirements paper that had been submitted. Detailed information regarding the implementation, as well as the virtual systems that were deployed, can be found in the sections below.

VIRTUAL HOSTS

The following hosts have been deployed into the Proof-of-concept environment:

DC01

This system will make use of it because it serves as the primary Domain Controller, DHCP server and DNS server for the augustacrissy.lab domain. The Vlan-SysAdmin and Vlan-Dev, and Vlan-Public networks each have their own set of static IP addresses that have been configured in place of DCHP. This server is the single source of truth to authenticate network resources.

Router

It acts as both a remote access point for users outside the virtual network as well as a significant gateway for the virtual network itself in this virtual environment.

IIS01 and IIS02

These virtual computers are equipped with the IIS webserver as well as the Remote Access Server software. In order to load balance requests and web requests on their common 10.0.1.10 IP address, the two remote network interfaces were configured as a team and then configured to load balance requests and web requests.

JMP01

This host, which serves as a gateway to internal services and systems, allows users to connect to other hosts via the Vlan-SysAdmin network.

NETWORKING

On a vSwitch that has been configured with port groups per VLAN, there is no external network adapter that has been chosen to assist in providing layer 2 isolation. Figure 1 (shown below) presents a list of the vSwitches and subnets that have been configured.

REMOTE ACCESS

During the system configuration process, the Company Overview and Requirements paper was scrupulously followed. The Remote Access Server role has been configured on both IIS01 and IIS02, and it is ready for usage by the tester and reviewer.

Host	Port Group	VLAN Tag	vNic	MAC	Host IF	IPv4
DC01	DEV	2	Network adapter 1	00:0c:29:7f:dd:33	Ethernet0	10.0.2.2
	SysADMIN	3	Network adapter 2	00:0c:29:7f:dd:3d	Ethernet1	10.0.3.2
Router	DEV	2	Network adapter 1	00:0c:29:05:3d:df	DEV (lan)	10.0.2.1
	Public	1	Network adapter 2	00:0c:29:05:3d:e9	PUBLIC (opt1)	10.0.1.1
	SysADMIN	3	Network adapter 3	00:0c:29:05:3d:f3	SYSADMIN (opt2)	10.0.3.1
	WAN	0	Network adapter 4	00:0c:29:05:3d:fd	WAN (wan)	
IIS01	Public	1	Network adapter 1	00:0c:29:93:c7:65	Ethernet0	10.0.1.3
	Public	1	Network adapter 2	00:0c:29:93:c7:6f	Ethernet1	10.0.1.4
	Public	1	Network adapter 3	00:0c:29:93:c7:6f	IIS01-Public-Team	10.0.1.8
	SysADMIN	3	Network adapter 3	00:0c:29:93:c7:79	Ethernet2	10.0.3.3
	DEV	2	Network adapter 4	00:0c:29:93:c7:83	Ethernet3	10.0.2.3
IIS02	Public	1	Network adapter 1	00:0c:29:81:d0:e9	Ethernet0	10.0.1.5
	Public	1	Network adapter 2	00:0c:29:81:d0:f3	Ethernet1	10.0.1.6
	Public	1	Network adapter 1	00:0c:29:81:d0:e9	IIS02-Public-Team	10.0.1.9
	SysADMIN	3	Network adapter 3	00:0c:29:81:d0:fd	Ethernet2	10.0.3.5
	DEV	2	Network adapter 4	00:0c:29:81:d0:07	Ethernet3	10.0.2.5
JMP01	Public	1	Network adapter 1	00:0c:29:3e:20:9b	Ethernet0	10.0.1.7
	DEV	2	Network adapter 2	00:0c:29:3e:20:a5	Ethernet1	DHCP
	SysADMIN	3	Network adapter 3	00:0c:29:3e:20:af	Ethernet2	10.0.3.7

Figure 1 IP/Subnet Assignment Table

C. SECURITY

For the purpose of protecting data and the network, the ISO/IEC 27001:2013 security strategy will be implemented. With this approach and certification, you'll be able to compete more effectively against your competitors, manage security costs more efficiently, and conform to state and federal requirements more effectively than before. Additional benefits include the successful protection of all confidential information, as well as the ability to improve corporate services and operations as a result of implementing this strategy

.

C.1. VIRUS SCAN SYSTEM

Unless needed by local, state, or federal legislation, it is not necessary to modify the default Windows Defender antivirus program installed on these computers. It is possible to push and deploy Window Defender virus definitions to all attached systems using the existing WSUS enterprise solution, and alarms may be configured to activate when threats or scan results are much higher than expected.

If your present antivirus solution has the capability of extending to the cloud, this is something you should explore. The assumption here is that there will be no additional licensing fees or restrictions incurred as a result of adopting the solution in this manner.

C.2. FIREWALL RULES

In Windows-based systems, Active Directory has the ability to and will enforce firewall rules to the greatest extent possible. Network-level controls for virtual infrastructure should be created and configured as needed using an automated configuration management framework, such as Chef, TerraForm, or Ansible, to ensure that they function properly. The principle of least privilege should be applied at all points of entry into a network, regardless of the type of access granted. The stateful firewall should be used whenever a decision must be made between a stateful and a stateless firewall, unless otherwise specified. As a result, outbound rule management will need less work on the part of the user.

Port	Transport Protocol	Session Protocol	DC01	IIS01	IIS02	JMP01
23	TCP	Telnet	DENY Telnet across the board because this isn't 1995			
All Outbound	All	All	ALLOW all outbound ports besides port 23 TCP Telnet			
53	TCP UDP	DNS	ALLOW	DENY	DENY	DENY
67	TCP UDP	DHCP	ALLOW	DENY	DENY	DENY
68	TCP UDP	DHCP	ALLOW	DENY	DENY	DENY
80	TCP	HTTP	ALLOW	ALLOW	ALLOW	DENY
443	TCP	HTTPS	ALLOW	ALLOW	ALLOW	DENY
3389	TCP UDP	RDP	ALLOW only SysAdmin VLAN DENY all others			DENY
All Other Inbound	All	All	DENY ALL			

C.3. ACCESS CONTROL LISTS

To implement Access Control, the principle of least privilege should be adhered to at all times. To ensure that only administrators have direct access to the underlying virtual infrastructure, administration credentials for virtual infrastructure should be maintained distinct from those used for normal servers or virtual appliances.

In order to gain granular control over the underlying resources that enable the virtual architecture, hosts should be domain-joined with the domain controller. If you wish to map Active Directory security groups to vSphere permission sets, you'll need to purchase business licenses for VMware's vSphere in order to accomplish this.

C.4. SECURITY GROUPS

Security groups in Windows should be extensively employed in order to adhere to the principle of least privilege. It is not recommended that security group memberships be concentrated in the hands of a single user. In order to ensure that a user truly need access to perform his or her responsibilities, documented user cases and requirements, as well as written approval from the user's manager or supervisor and the office of the CISO, should be obtained prior to participation in a Security Group.

C.5. INFORMATION SECURITY MANAGEMENT

We anticipate that the virtual system and infrastructure will adhere to all existing and applicable company standards. The finished result must either fulfill or exceed the current ISO/IEC 27000:2018 or the ISMS criteria, whichever is higher in terms of quality. Virtualization specialists should be a significant component of the security management team of Augusta Crissy Detective Games, and they shall be responsible for ensuring that the requirements outlined in this document are fulfilled or exceeded. It would be the responsibility of the new role to ensure that protections for the new virtual network get incorporated into the company's current information security management standards (ISMS). The new ISMS guidelines must take into consideration all of the various components.

D. IMPLEMENTATION PROCESS

The following milestones must be satisfied in order to proceed through the steps of the overall implementation.

Phase	Milestone	Dependency
Phase 1	Choose a Cloud Service Provider, and then Create a backup strategy and, if necessary, select a backup service provider to implement it.	Examine whether the service provider is capable of adhering to the organizational standards and security frameworks required for a hybrid cloud datacenter.
Phase 2	The infrastructure for networking has been set up, configured, and secured, as well as the network itself.	ACL and firewall setups, VLAN assignments, domain names, IP subnetting, and DNS.
Phase 3	Active Directory, Remote Access, and Proxy Servers are tested and verified to function properly.	Create a test user base and establish VPN profiles and encryption standards so that you can beta test a few servers before launching them into production.
Phase 4	IIS Datacenter Servers, NICS Team, and load balancing should all be put in place.	Check the ping of the Team NICs and the NLB-Cluster to ensure that everything is operational. Determine whether IIS is functioning properly.
Phase 5	Validation of VPN and RDP connections both internally and externally	Remote Desktop is enabled on all of the servers in the datacenter, and the VPN has been properly configured.

Phase 1

Select a Cloud Service Provider that will meet the needs of Augusta Crissy Gaming and commit to working with them until completion of the job. Then devise a plan for what to do if something does go wrong. Determine a backup service provider who will be in charge of carrying out the strategy's implementation if it becomes necessary at the eleventh hour. Inquire about the service provider's willingness and capacity to conform to the organizational standards and security frameworks required for a hybrid cloud datacenter.

Phase 2

The next goal is the installation, setup, and security of both the physical network infrastructure and the configuration of the virtual network infrastructure. At this point, the work consists of an access control list and firewall configurations, VLAN assignments, DNS and domain configuration, and IP subnetting, among other things.

Phase 3

Before being deployed, Active Directory, Remote Access, and Proxy Servers are tested and validated to ensure that they are in working order. An administrator must first construct a test user base and then generate VPN profiles and encryption standards to beta-test many servers before bringing them into production mode.

Phase 4

All necessary components, including IIS Datacenter Servers, teamed network interface cards, and network load balancing clusters, should be in place. In order to ensure that everything is working correctly, check the ping of the teaming NICs and the NLB cluster. Verify that the IIS server is up and running correctly.

Phase 5

All of the datacenter's servers are equipped with a remote desktop connection, as well as a VPN that has been appropriately configured. Last but not least, an administrator should verify VPN and RDP connections both internally and externally.

E. PERFORMANCE TUNING

In order to address performance concerns, a plethora of performance tuning options is available in Windows 2019. Network Interface Teaming was one of these tools developed to improve network performance. In order to enhance throughput to and from the server, it is necessary to establish Network Teaming over a large number of physical network adapters.

If the primary host fails or becomes inaccessible, an admin can use VMware's vMotion feature to relocate the virtual machines to another physical server if a primary ESXi host is unavailable. As a result of this feature, the virtual environment is never interrupted by hardware failures or network disruptions.

The following are some places to start exploring to determine where performance issues originate. VMware Performance Monitoring provides detailed real-time data through the vSphere client. An admin can log into the ESXi interface setup, a vCenter server, or the vSphere Client and navigate to any VM experiencing poor performance to examine the resources assigned versus the resources consumed. If the vMEM or vCPU resources are approaching their limitations, it will be required to increase them in order to avoid a VM bottleneck due to host resource contention.

Also, by logging into the guest operating system and viewing the Resource Monitor or Task Manager, an admin can discern which apps consume excessive resources. Performance Monitor can be used to track network error rates over time by logging information such as Network Adapter Errors Received and Network Adapter Bytes Received, CPU, Disk Queue, and Memory Errors per second. These metrics will inform an admin of the rate at which the VM's resources are consumed or may reveal other bottlenecks in the pipeline.

F. LOAD BALANCING

When it comes to gaming assets, full cloud solutions may and should be used. Localizing load balancing, on the other hand, does not provide the same advantages as employing a cloud-based solution, such as scale, simplicity, low overhead, and a broad variety of configuration possibilities. Network load balancers can be put upstream of gaming servers, and client location, IP addresses, and request types can all be utilized to determine where traffic will be shaped and balanced across the target application/server. This allows for the implementation of Google Cloud Platform, AWS, or Azure. Following the load balancing choice, the metrics recognized by the decision can then be used to provide real-time advice on necessary measures to correct any load balancing challenges on the virtual infrastructure.

TESTING STRATEGY

Test 1: Connect a few testers to the gaming system via a load balancer, and then power cycle the system on which they are currently logged in to mimic a server outage.

Acceptance Criteria: For as long as the load balancer is in charge of keeping things balanced, there should be no significant service outages for the users.

Test 2: Connecting two people from separate locations to the game system for testing purposes is recommended. In order to find the best testers, the systems should be accessed from as far away as possible, such as from the east and west coasts, or the far north and south-central United States.

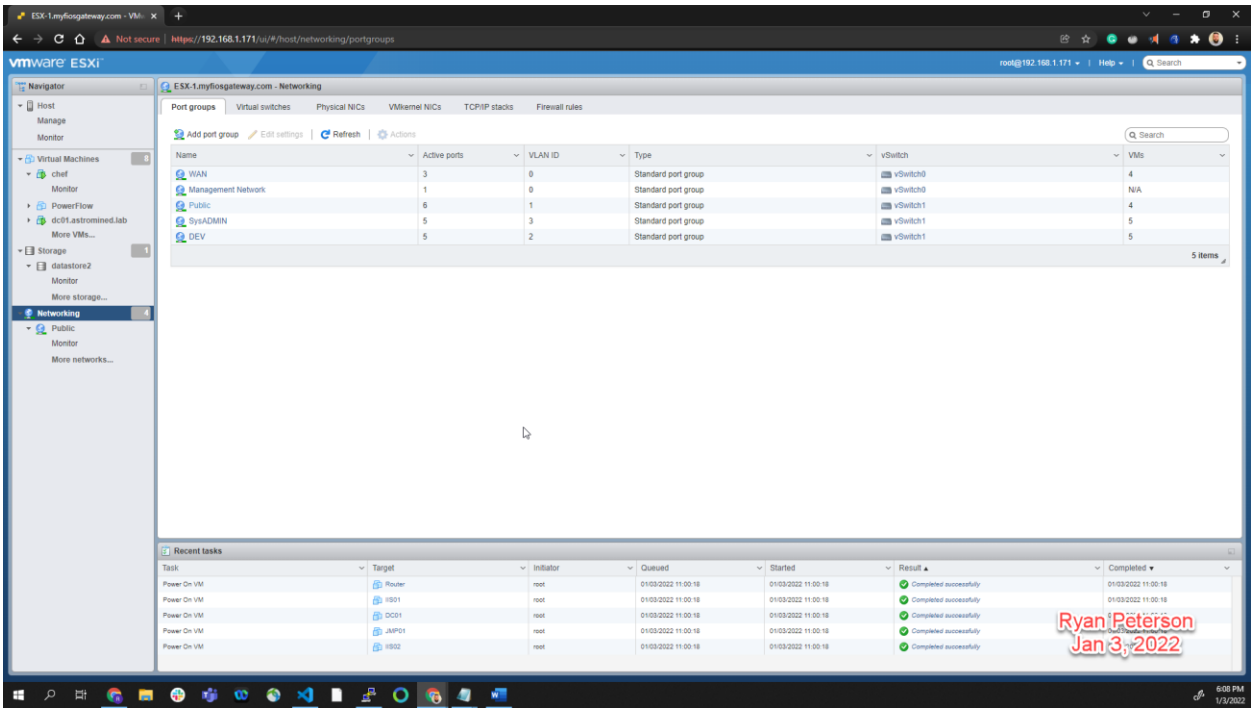
Acceptance Criteria: Each user has the same latency across all of his or her connections to the load balancer.

G. PROOF-OF-CONCEPT IMPLEMENTATION BUILD

Each phase of implementation has been documented with a screenshot and a brief discussion of how it was accomplished in the lab environment.

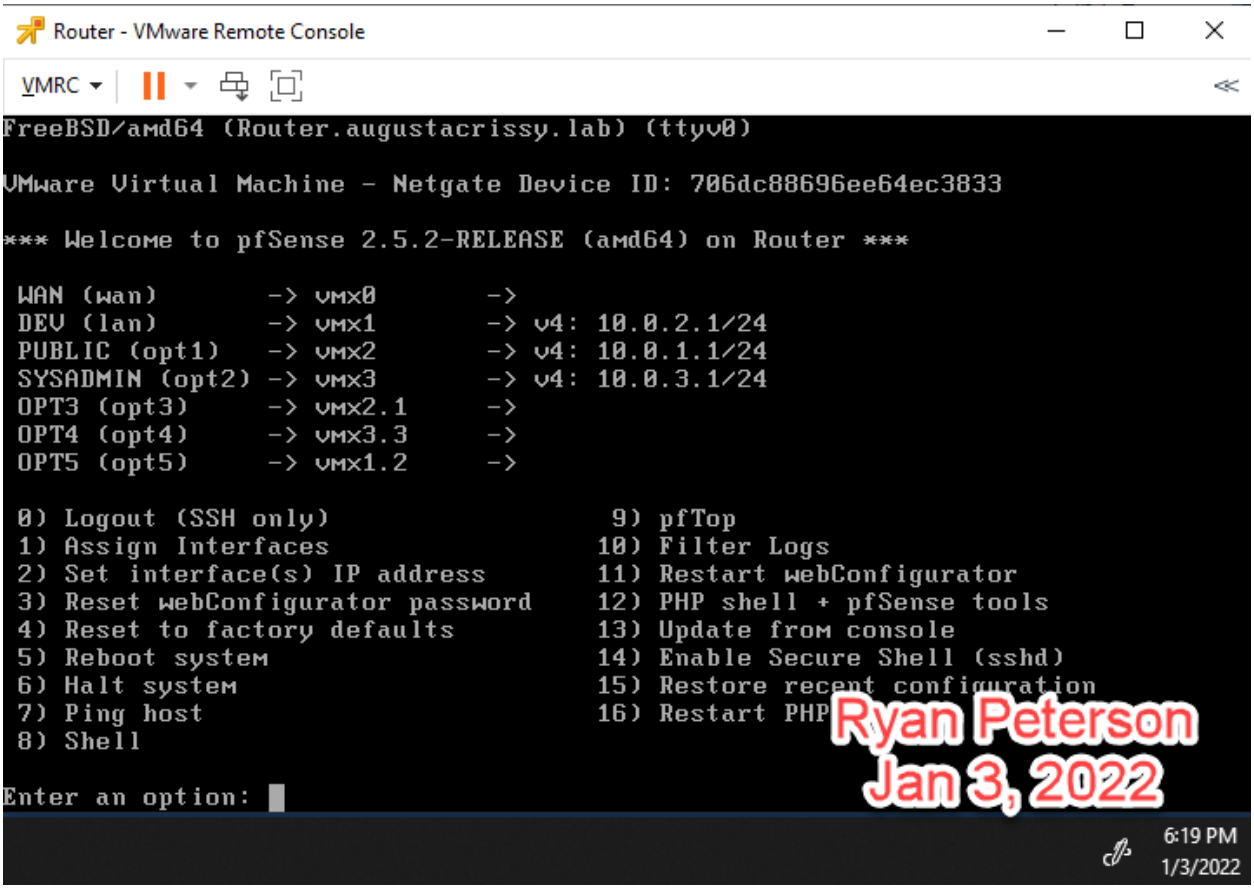
G.1. PHASE 1

This Proof of Concept was carried out using VMware ESXi 6.7 on a Dell PowerEdge R720 server in my home-lab testing environment. For a full Datacenter Virtualization Solution, Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform are the most suitable options available.

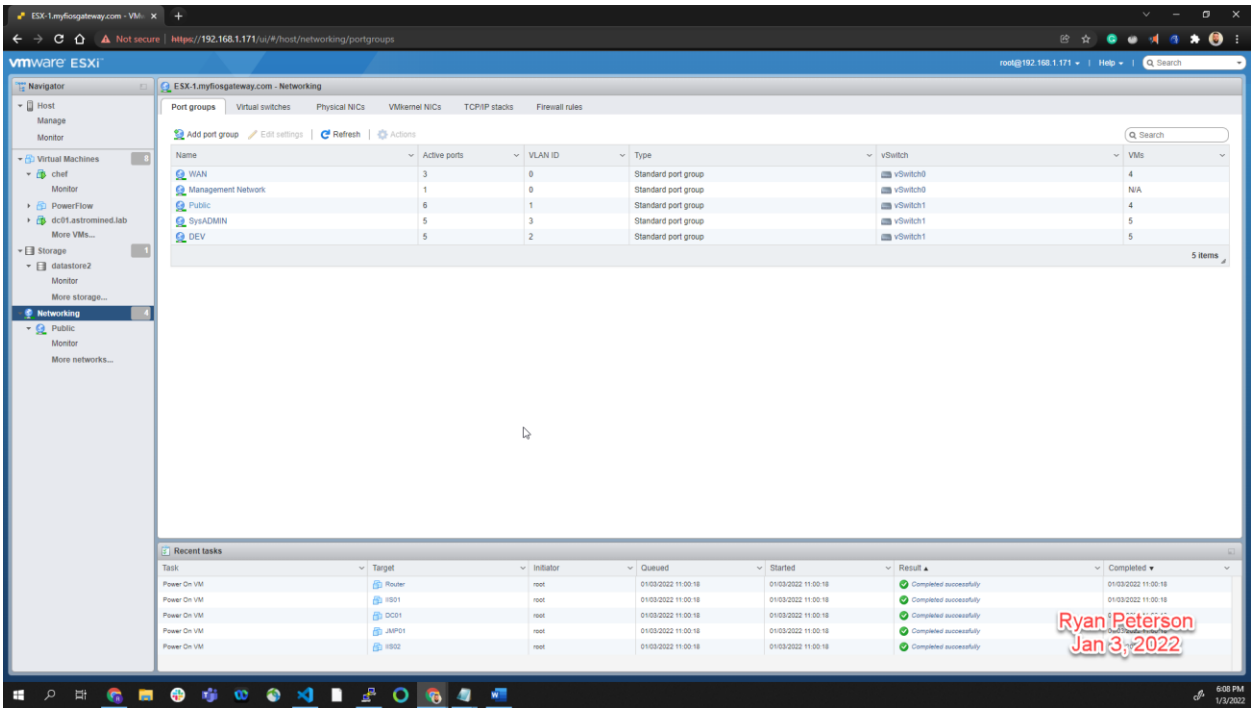


G.2. PHASE 2

This allows you to see the pfSense Router Appliance, which was configured to act as a gateway for traffic entering and exiting the virtual network. Here is the view of the VLANs from the router, showing their IF names and subnets:

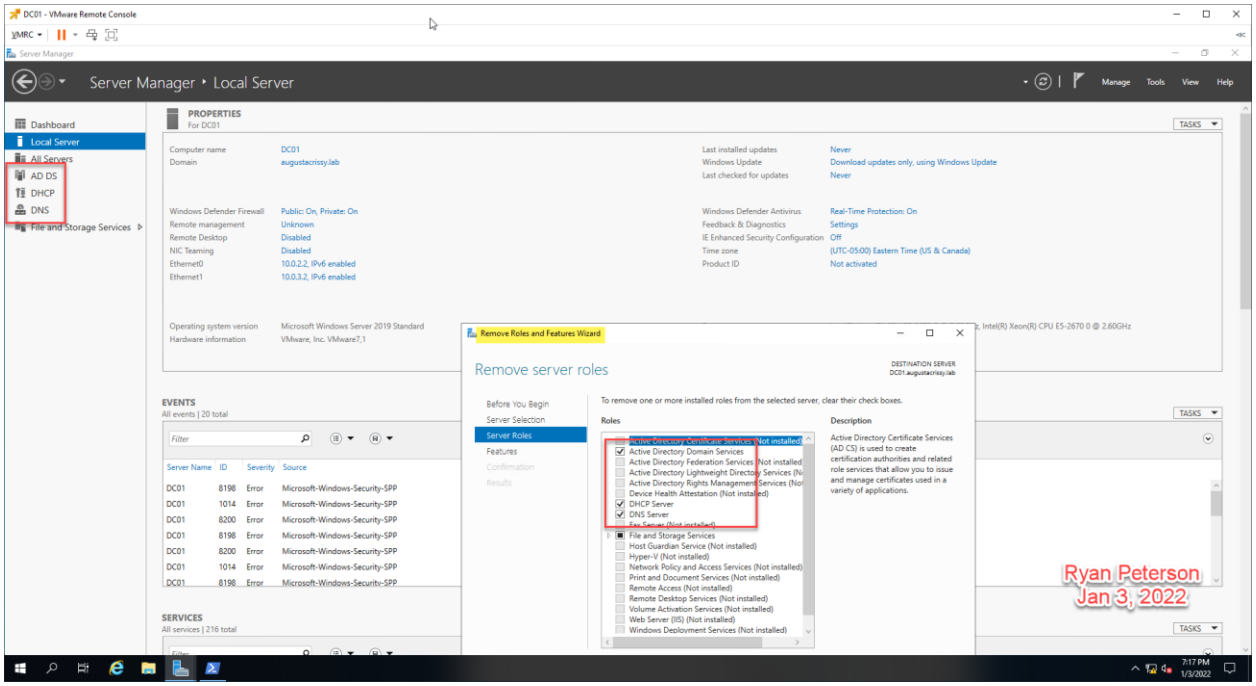


Several port groups are assigned to 2 virtual switches, which are used by the VMs to divide their LAN segments. With my local network configuration and firewall setup, I needed the WAN port group to have a separate vSwitch to ensure the integrity of my network.



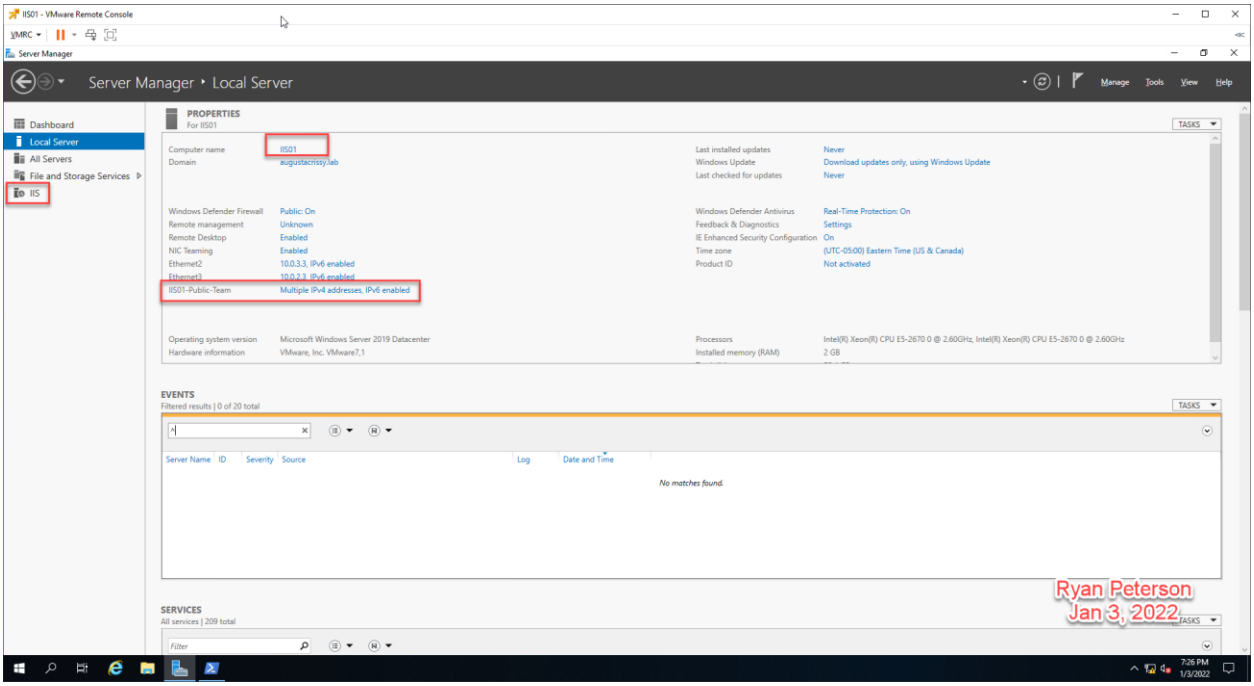
G.3. PHASE 3

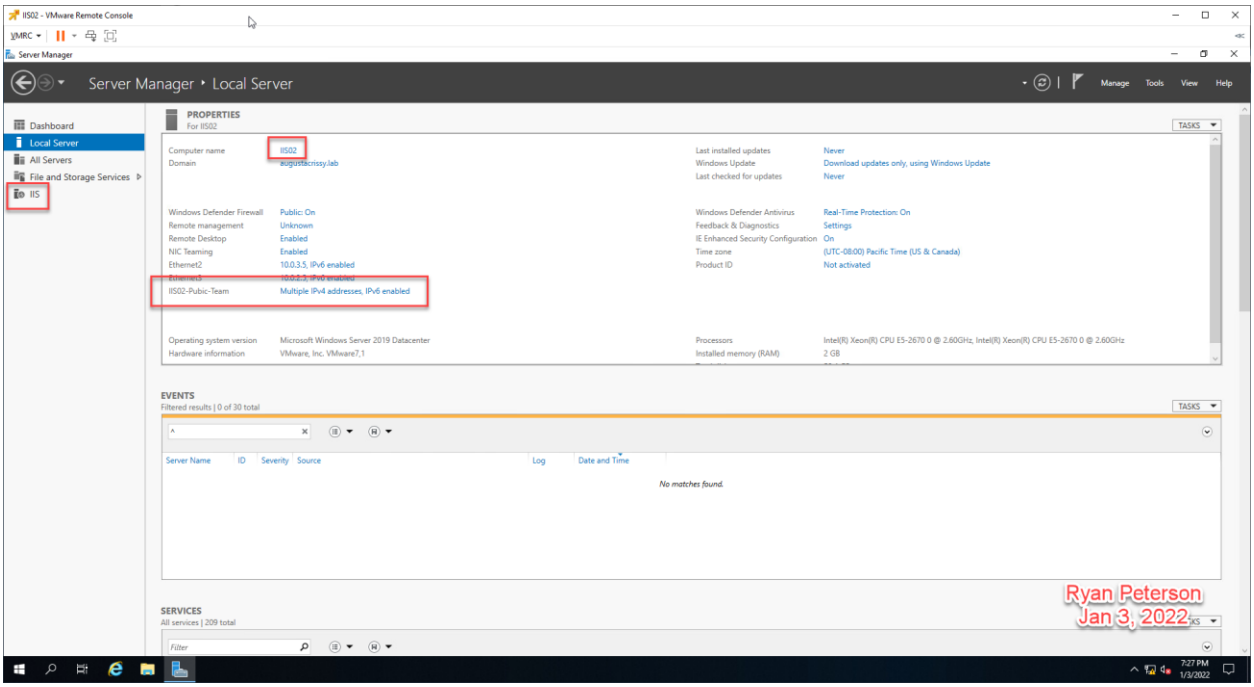
This screenshot, which was taken from the Windows 2019 Standard server host DC01, shows that Active Directory, DNS, and DHCP were configured for the AD Domain.



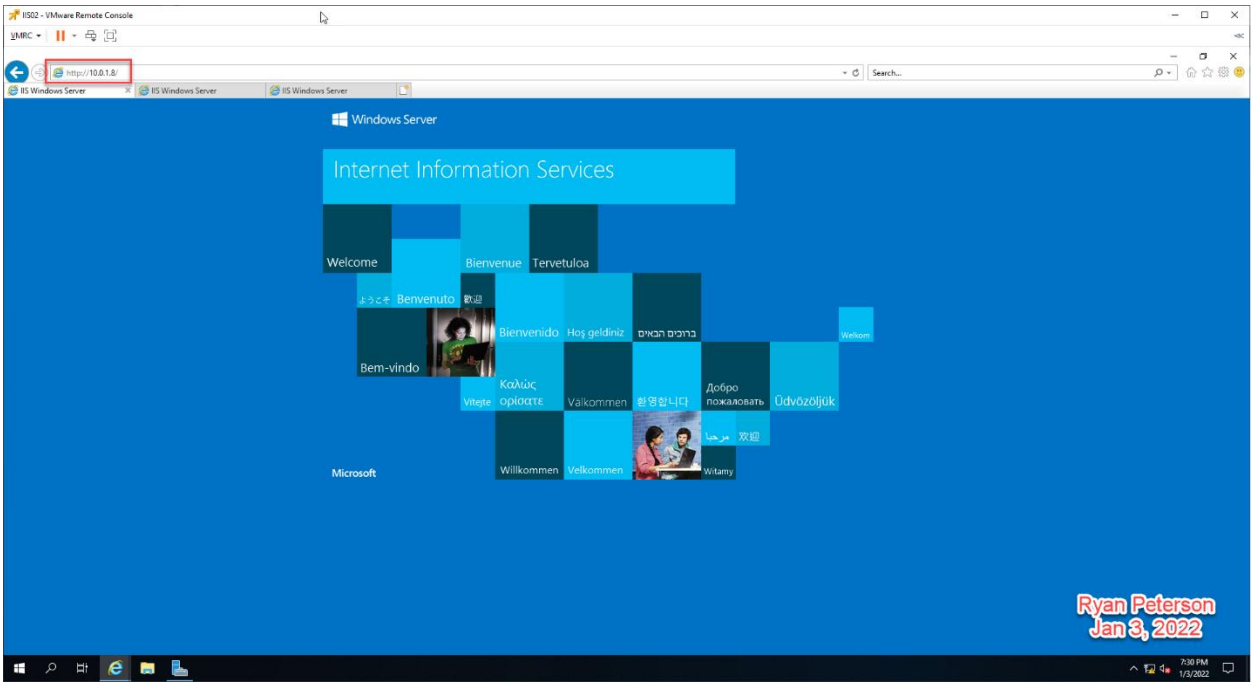
G.4. PHASE 4

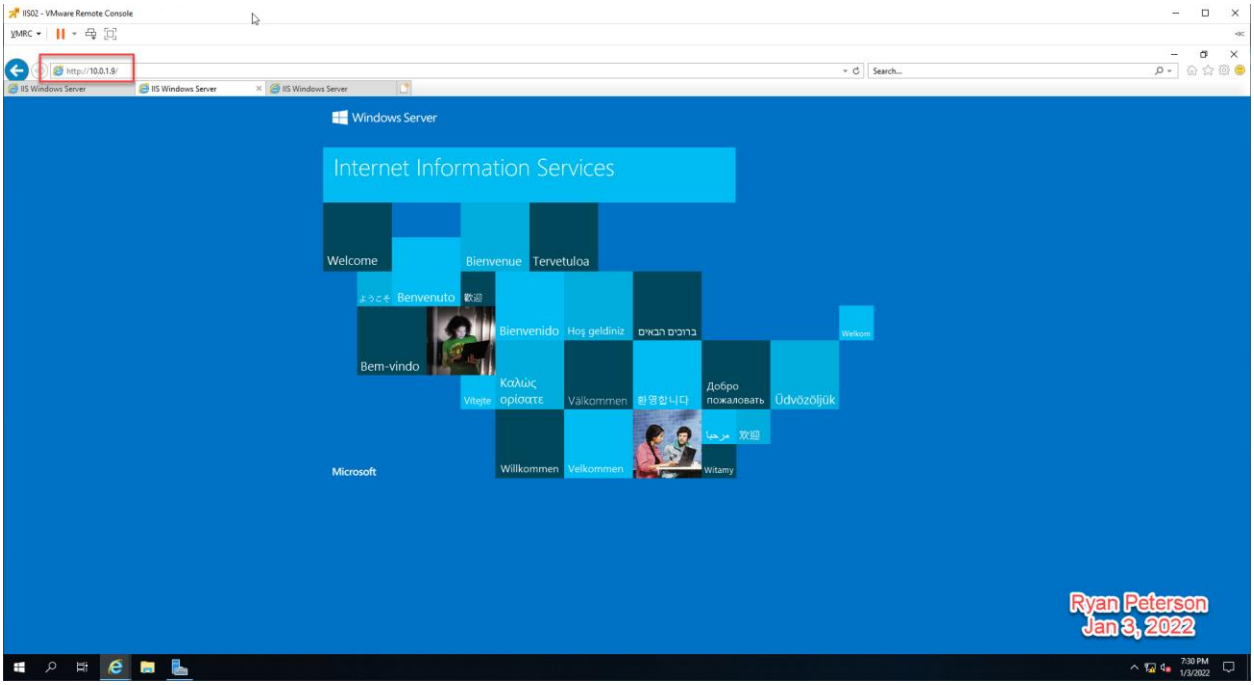
IIS has been installed on IIS01 and IIS02 and 2 interfaces on each host have been configured as a nic team.





IIS Default site function for IIS01's nic team IP of 10.0.1.8, IIS02's nic team IP of 10.0.1.9, along with the NLB's virtual IP of 10.0.1.10.





Network Load Balancing has been configured for the nic teams on IIS01 and IIS02, with a virtual IP of 10.0.1.10.