**Design Template**

|  |
| --- |
| Augusta Crissy Detective Games |
| Proof-of-Concept Design Template |
| Datacenter Virtualization Proof of Concept |

|  |
| --- |
| name  [Date]  [Version 1.1] |

Contents

[A. Systems Analysis of Current ENvironment 3](#_Toc14092364)

[B. Virtualization Solution 4](#_Toc14092365)

[C. Security 5](#_Toc14092366)

[C.1. Virus Scan System 5](#_Toc14092367)

[C.2. Firewall Rules 5](#_Toc14092368)

[C.3. Access Control Lists 5](#_Toc14092369)

[C.4. Security Groups 5](#_Toc14092370)

[C.5. Information Security Management 6](#_Toc14092371)

[D. Implementation Process 7](#_Toc14092372)

[E. Performance Tuning 8](#_Toc14092373)

[F. Load Balancing 8](#_Toc14092374)

[G. Proof-of-Concept Implementation Build 9](#_Toc14092375)

[G.1. Phase 1 9](#_Toc14092376)

[G.2. Phase 2 9](#_Toc14092377)

[G.3. Phase 3 9](#_Toc14092378)

[G.4. phase 4 9](#_Toc14092379)

# Systems Analysis of Current ENvironment

With Augusta Crissy Detective Games’ new role-playing games becoming ever more popular and virtual reality one of the current hot topics with gaming the trends are reflecting that the datacenter needs to move to a more virtual environment. The reasons behind this are the current limitations of their current datacenter which is constrained by its size, power rating and cooling abilities. With virtualization in a hybrid-cloud datacenter solution they would gain additional server space and capacity on top of their current physical infrastructure.

The hybrid cloud solution would give them the expansion needed without the costs of real estate investment or leasing, the ability to expand quickly with demand, and the cost of having to purchase new hardware would be negligible compared to the cost of having to buy server hardware along with datacenter floor space. With virtualization there are many options where the server space is leased with options to expand the moment demand peaks and new virtual servers can be added to the domain in a matter of hours instead of days to weeks when having to wait for hardware and then having to build the system before it is ready to be put into service.

# Virtualization Solution

Describe a proposed configuration solution to meet the business and technical requirements outlined in the “Company Overview and Requirements” attachment.

The virtualization solution will be deployed on an ESXi host in strict compliance with the outlines company required detailed in the Company Overview and Requirements document. Special attention was given to each individual requirement to ensure that the proposed solution not only fits the need but also fulfills all requirements.

**HOW THE SOLUTION MEETS THE BUSINESS NEEDS**

This proof of concept outlines some of the benefits of datacenter virtualization and therefore should provide an adequate demonstration showing the merits of virtualization technologies. In order to fully meet the business needs this solution should be deployed alongside a vSphere Datacenter, this would enable full active directory integration and larger feature sets than available in the free version of ESXi.

**HOW THE SOLUTION MEETS THE TECHNICAL REQUIREMENTS**

The deployed proof of concept followed the requirements outlined in the provided requirements document. Below that are the detailed specifics of the implementation and virtual systems deployed.

**VIRTUAL HOSTS**

The following are the hosts that will be deployed into the environment:

**Srv19-Standard**

This system will act as the Domain Controller and Primary DNS server for augustacrissy.lab. It is configured with DCHP to issue IP addresses for both the Vlan-SysAdmin and Vlan-Dev networks. It also acts as a single point of authentication to network resources.

**pfSense ROUTER**

This virtual appliance has been configured to as the remote access endpoint to the network as well as the main gateway for the virtual environment and network.

**Srv19-DC1 and Srv19-DC2**

These virtual machines are configured with IIS webserver and Remote Access Server. The 2 network interfaces that are accessible remotely have been configured in a team and then configured to load balance requests and web requests on their shared IP address of 172.17.0.4.

**Win10-Ent**

This is acts as a gateway host for access to internal services and systems.

**NETWORKING**

A vSwitch will be deployed per VLAN without an external network adapter assigned to help in assisting layer 2 isolation. The vSwitches and subnets the support are shown below in B.2. IP/Subnet Assignments.

**REMOTE ACCESS**

The outlined configuration in the Company Overview and Requirements document has been followed closely with the only exception being it was deployed via OpenVPN server deployed on the pfSense Router appliance. The RAS role was still installed to Srv19-DC1 and Srv19-DC2 and fully functional should the tester and reviewer require them.

**IP/SUBNET ASSIGNMENTS NETWORK DIAGRAM**

Static IP addresses assigned to the virtual hosts are listed here and setup to allow for maximum control over the network and security allowing full monitoring of all internal and external traffic on the network.



* 1. Proof of concept – Datacenter Virtualization implementation diagram

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Host** | **Interface** | **IP** | **VLAN** | **vSwitch** |
| Svr-19-Stanard | Eth0 | 172.17.0.2/16 | dev | Vlan-DEV |
|  | Eth1 | 172.18.0.2/16 | sysadmin | Vlan-SysAdmin |
|  |  |  |  |  |
| pfSense | Em0 | 172.19.0.0/24 | Public | Vlan-pfSenseWAN |
|  | Em1 | 172.16.0.0/24 | Dev | Vlan-pfSenseLAN |
|  |  |  |  |  |
| Srv-Datacenter1 | Eth0 | 172.16.0.107/24 | lan | Vlan-pfSenseLAN |
|  | Eth1 | 172.16.0.108/24 | lan | Vlan-pfSenseLAN |
|  | Eth2 | 172.18.0.4/16 | SysAdmin | Vlan-SysAdmin |
|  | Eth3 | 172.17.0.4/16 | Dev | Vlan-DEV |
|  |  |  |  |  |
| Srv-Datacenter2 | Eth0 | 172.16.0.109/24 | lan | Vlan-pfSenseLAN |
|  | Eth1 | 172.16.0.110/24 | lan | Vlan-pfSenseLAN |
|  | Eth2 | 172.18.0.5/16 | SysAdmin | Vlan-SysAdmin |
|  | Eth3 | 172.17.0.5/16 | Dev | Vlan-DEV |
|  |  |  |  |  |
| Srv19-DC1 and Srv19-DC2 LoadBalancer |  | 172.17.0.4 |  |  |
|  |  |  |  |  |
| Win10-Ent | Eth0 | 172.17.0.3/16 | dev | Vlan-DEV |
|  | Eth1 | 172.18.0.3/16 | sysadmin | Vlan-SysAdmin |
|  | Eth3 | 172.19.0.3/16 | wan | Vlan-pfSenseWAN |
|  |  |  |  |  |
| ESXi Server Host |  | 172.16.0.213 |  |  |

B.2 IP/Subnet Assignment Table

# Security

Describe a security plan for this migration for *each* of the following requirements:

TO protect the data and network the security plan that will be implemented will be an ISO/IEC 27001:2013 plan. With this plan and certification there is a greater value add to fight competitors, have efficient security cost management and comply with local and federal laws. This plan will also effectively ensure that all confidential data is secure, and this process can be used to improve services and processes within the company.

*Note: All subsections are required. Refer to the requirements section and rubric section of the assessment for additional information.*

# Virus Scan System

Unless local, state or federal regulations require an alternative solution, the default windows defender antivirus solution can be utilized. The virus definitions for window defender can pushed and deployed to all attached systems via the existing WSUS enterprise solution and alerts can be configured to trigger for higher than the usual threats/scan results.

An alternative would be to use the existing enterprise A/V solution if it has an option to extend into the cloud environment. This of course assumes that there are no additional licensing costs or constraints in utilizing the solution int his way.

# Firewall Rules

Firewall rule can and will be fully enforced via active directory on the windows based systems. The implementation of an automated configuration management framework (JuJu, Pulumi, TerraForm or similar) should be utilized to ensure that networking level controls on the virtual infrastructure are enforced and configured as applicable. At all point of ingress into the networking the principles of least privilege should be enforced. When a decision to choose a stateful or stateless firewall is to be made, a stateful should be the chosen firewall. This will reduce the overhead required for outbound rule management.

# Access Control Lists

Access Control should be enforced via the principles of least privilege. The only persons who should have direct access to underlying virtual infrastructure are administrators and the virtualization credentials should be separate from that of the standard servers or virtual appliance credentials.

Granular control over the underlying resources providing the virtual infrastructure should be achieved by the hosts being domain joined. For this to be achieved enterprise licenses would need to be purchased for VMware’s vSphere, this would allow for the mapping of Active Directory security groups with vSphere defined permission sets.

# Security Groups

The security groups within windows should be utilized to their fullest to support principles of least privilege separation of duties. There should be no one person who would be a “super” user and have absolute control over security group memberships. Security Group membership should have a documented user case and need along with written approval of the user’s supervisor/manager and the ISSO to ensure that the user actually requires the access for job function.

# Information Security Management

The virtual system and infrastructure will adhere to all current and applicable company standards that are currently in place with the organization. The final deliverable should adhere to or exceed the ISO/IEC 27000:2018 current ISMS standards. To ensure that the standards outlined in this publication are met or exceeded Augusta Crissy Detective Games should expand their current security management team to include a virtualization specialization member. The new role would be responsible for expanding the current ISM guidelines within the company to include provisions for the new virtual network. All element aspects should be considered and accounted for in the new ISMS guidelines.

# Implementation Process

|  |  |  |
| --- | --- | --- |
| Phase | Milestone | Dependency |
| Phase 1 | Choose Cloud Service Provider, Design Backup Solution, and Choose Backup Provider if needed | Research on which service provider can align with the organizational standards and security frameworks required for hybrid-cloud datacenter. |
| Phase 2 | Networking infrastructure deployed, configured and secured. | IP subnetting, VLAN assignments, domain names, firewalls and ACL designs. |
| Phase 3 | Active Directory, Remote Access, Proxy Servers tested and verified are functional | Set up of VPN profiles, encryption standards and create a test user-base to beta test few servers. |
| Phase 4 | Deploy IIS Datacenter Servers, Team NICS and Load Balance. | Verify IIS operational, Validate Ping of Team NIC’s, Validate NLB-Cluster. |
| Phase 5 | Validate VPN, RDP Internally and Externally | Remote Desktop Enabled on Datacenter Servers, VPN configured Correctly on Datacenter Servers |

# Performance Tuning

Windows 2019 offers many options for performance tuning and that relate to performance issues; Network Teaming was one such option that was implemented to increase performance on the network. With Network Teaming implemented across multiple physical network adapters, network traffic is spread out thus increasing throughput to and from the server.

Another option is to implement VMware’s vMotion to migrate live virtual machines to a new physical host in the event of a failure on the primary or outage. This feature helps to ensure there are no outages of the virtual environment due to hardware failures or outages.

To determine the origin of performance anomalies that are to main locations to look. The guest operating system or VMware Performance Monitoring. To address the first, you would need to login to the guest OS and user Resource Monitor/Task Manager to see if there are any items using excessive resources at a quick glance.

You can also use Performance Monitor in the long term for logging of details such as Network Adapter Errors Received vs Network Adapter Bytes Received to check the network error rate, CPU Disk Queue to see how long programs are needing to wait to write to the disk, or Memory Errors/sec let you know how fast the memory in the is degrading.

To address the second, you would need to log into the ESXi interface setup, the ESXi host web access portal or the vSphere Client, navigate to the VM with poor performance and check the resources assigned vs resources consumed. If the vMEM and vCPU are at capacity, then they would need to be increased otherwise it could be a bottleneck within the VM itself.

# Load Balancing

Assets utilized in gaming can and should be deployed to full cloud solutions. Localizing load balancing is possible but not at the scale, simplicity, low overhead, variety of options available in a cloud-based load balancing solution. Let’s assume that the game assets are deployed to Google Cloud Platform, network load balancers can be placed upstream to the gaming servers and client location, IP addresses, and request types can all the used to determine where and how the traffic would be shaped and balanced across the target application/server. The metrics realized by the load balancing decision can then be passed to s3 and vROPs to assist in real time suggestions for necessary actions to fix any load balancing issues that may arise on the virtual infrastructure.

**TESTING STRATEGY**

**Test 1:** Have a few testers login to the gaming system via a load balancer and power cycle the system that they are currently on to mimic a physical outage of the server.

**Acceptance Criteria:** The users should be automatically migrated to a healthy host backed by the load balancer and should not see a major disruption in service.

**Test 2:** Have 2 test users connect to the gaming system from alternate locations. Ideally, they should connect to the systems from as far away as possible, like the east coast and west coast, or as far north and south as possible to find testers.

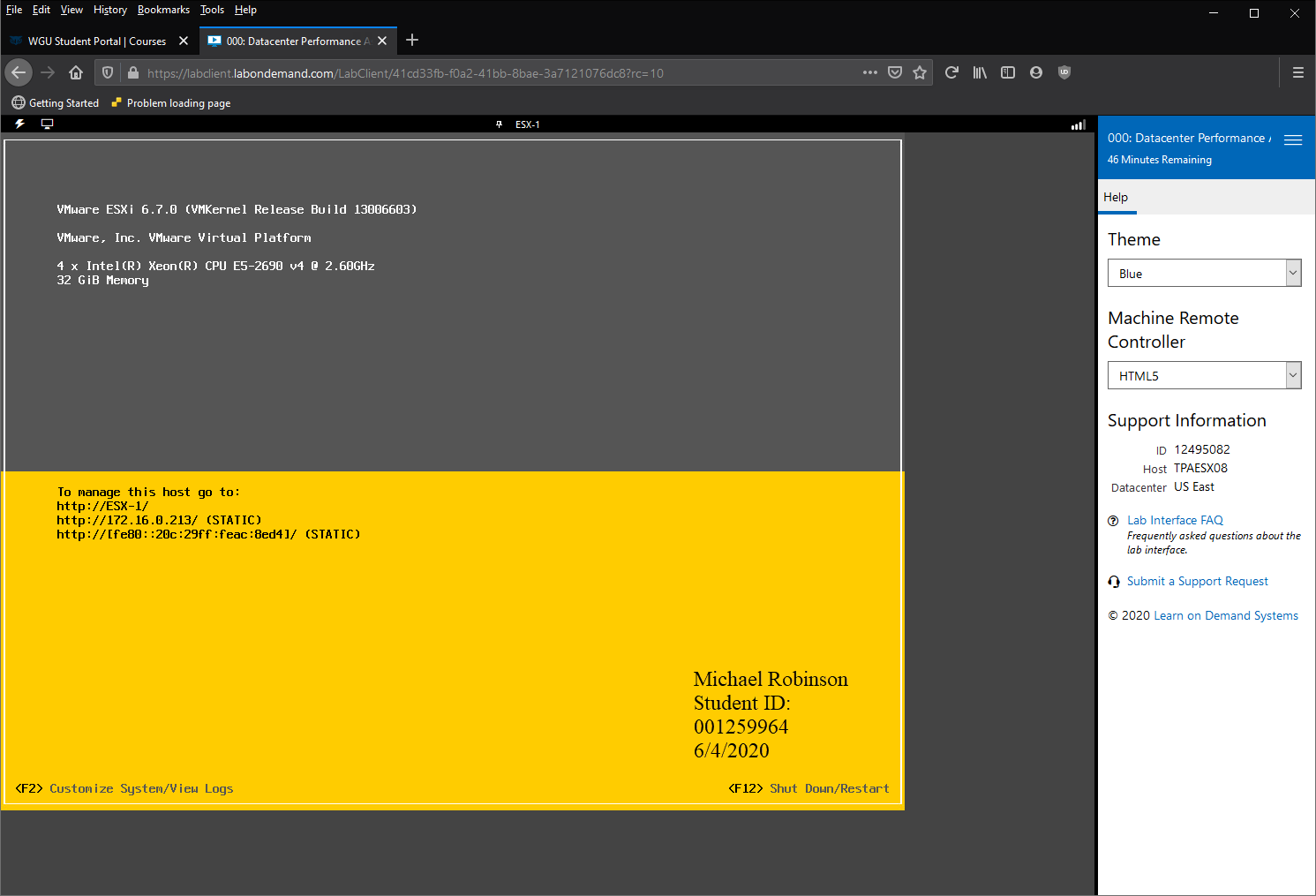
**Acceptance Criteria:** Each user experiences the same latency across their respective connections into the load balancer.

# Proof-of-Concept Implementation Build

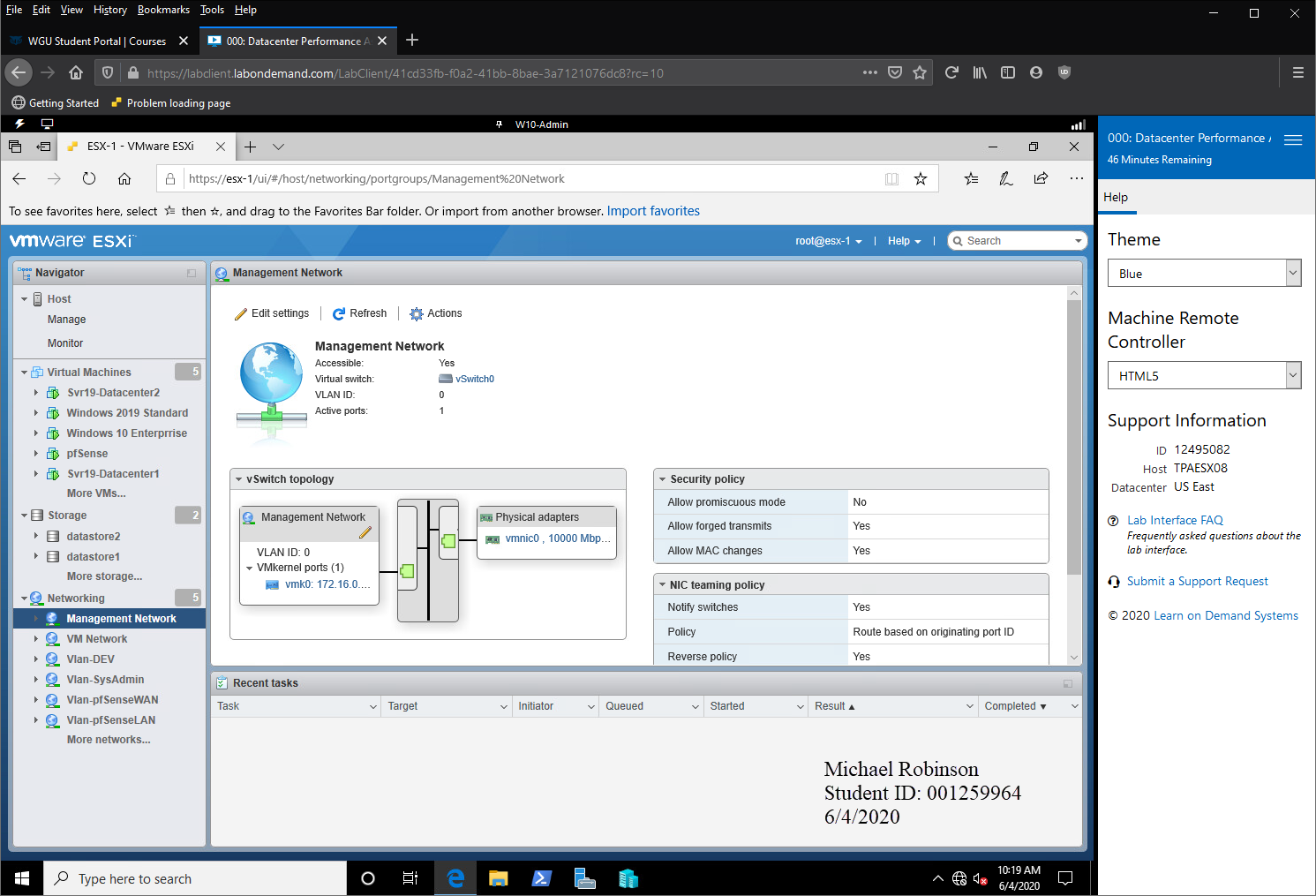
Provide a separate screenshot of *each* implementation phase completed in the lab environment, including a brief explanation of the process.

# Phase 1 - Cloud Service Provider, Backup Solution

For this Proof of Concept VMware ESXi 6.7 was utilized. For a full Datacenter Virtual Solution Amazon AWS or Google Cloud Platform should be utilized.

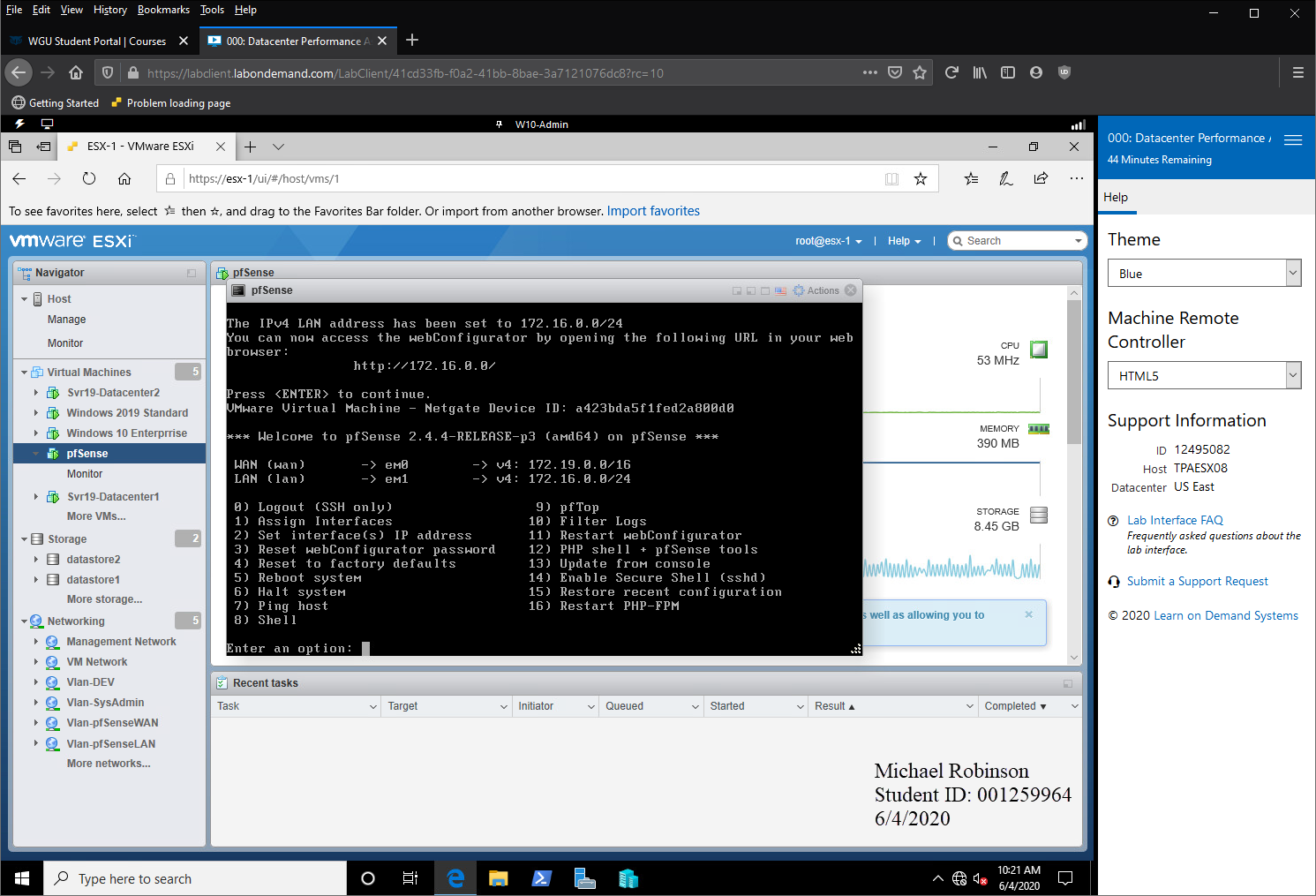


This screenshot reflects the ESXi interface for the virtual Proof of Concept that houses all the virtual machines.

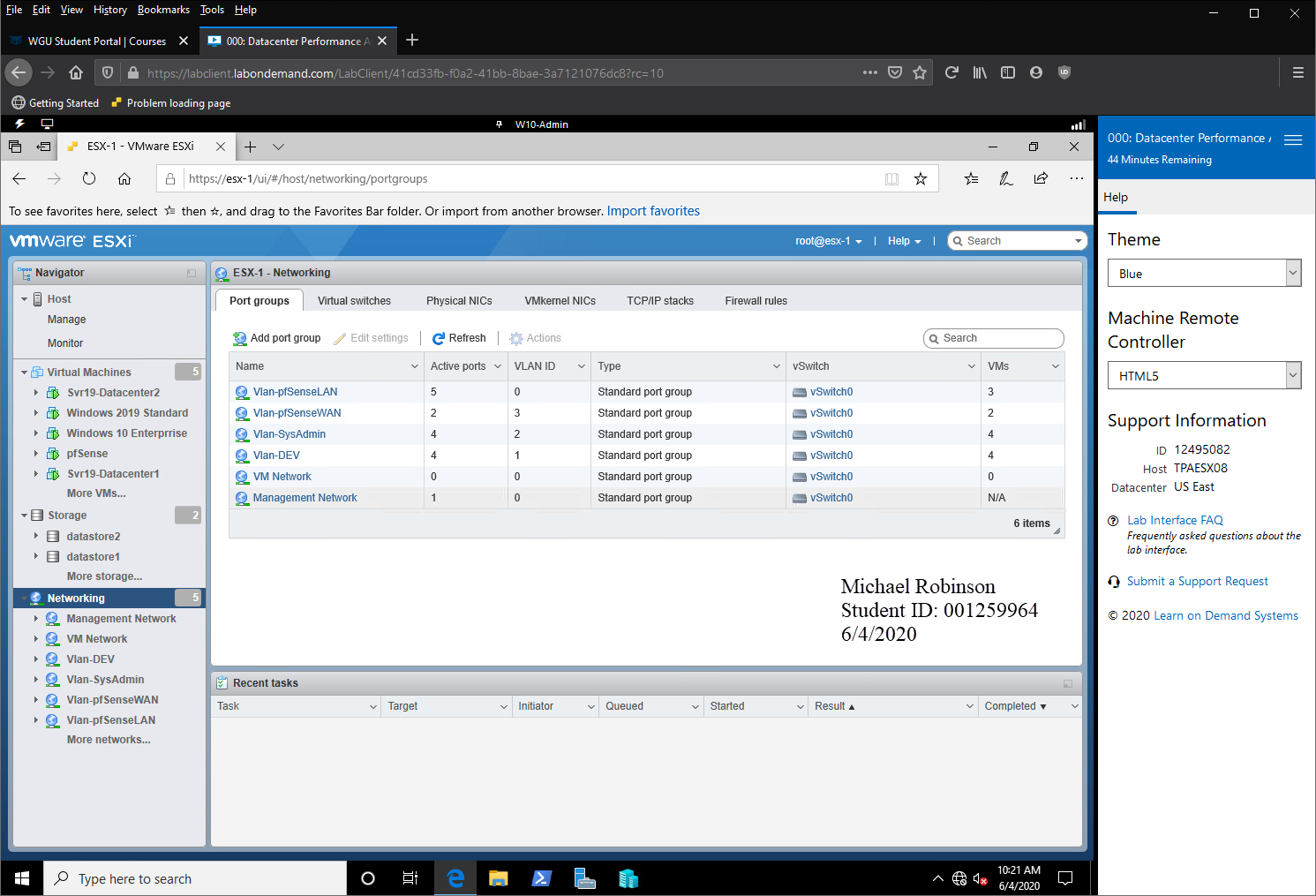


Here you can see the web interface of the ESXi host with all the VM’s, Datastores, and Virtual Switches that comprise the virtual environment.

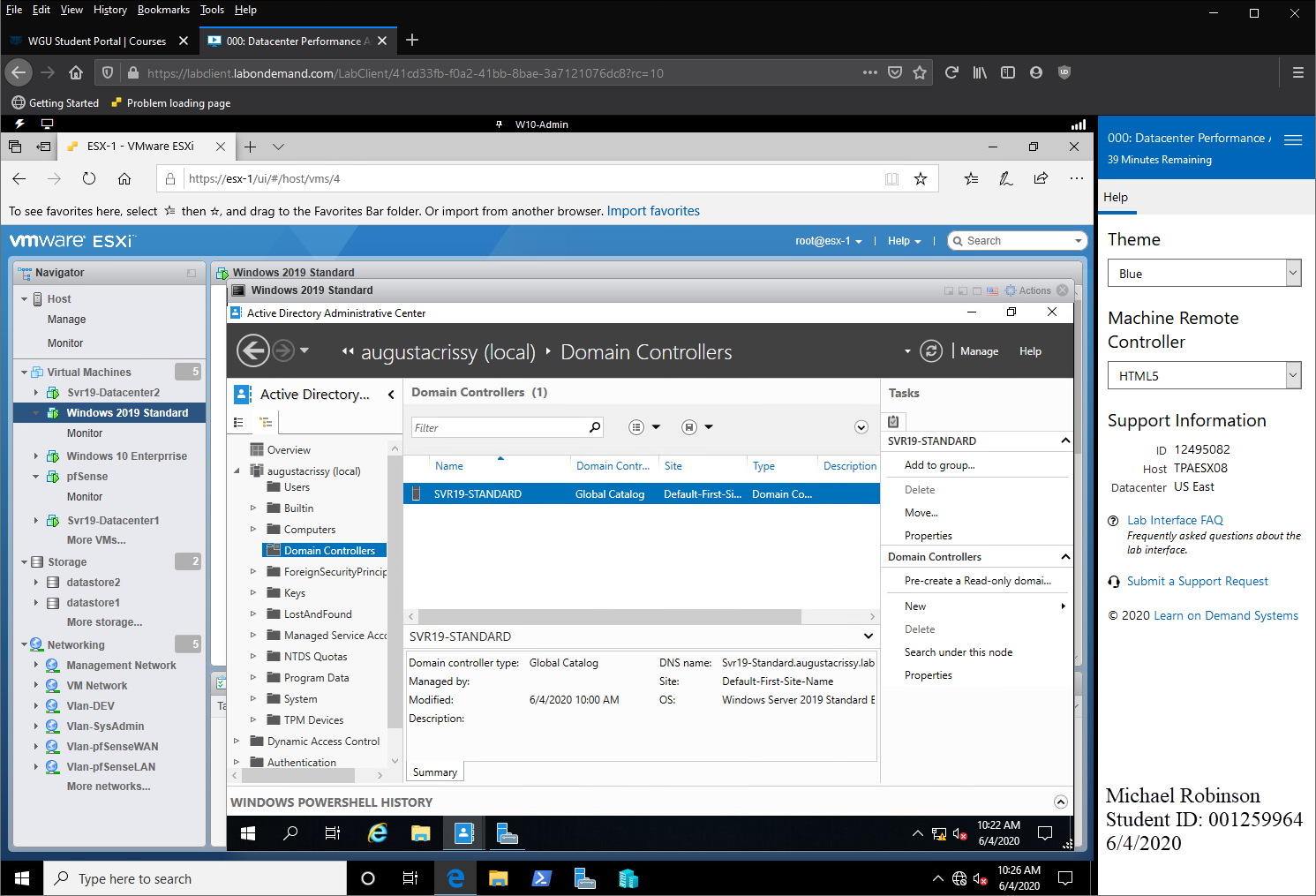
# Phase 2 - Networking infrastructure deployed, configured and secured



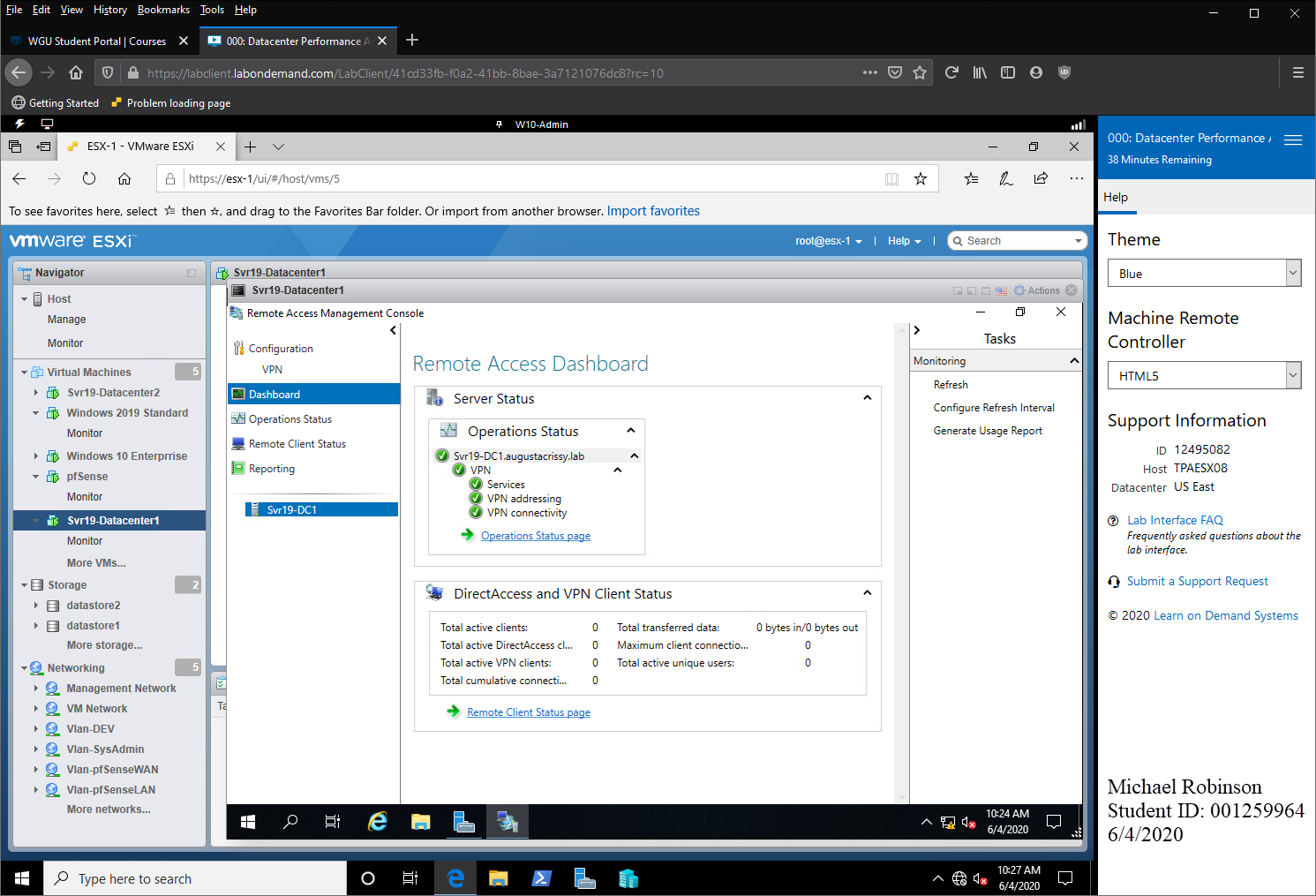
With this you can see the pfSense Router Appliance that was deployed to act as a gateway into the and out of the virtual network.

  
This screenshot shows the different virtual switches used by the VMs for LAN segment separation.

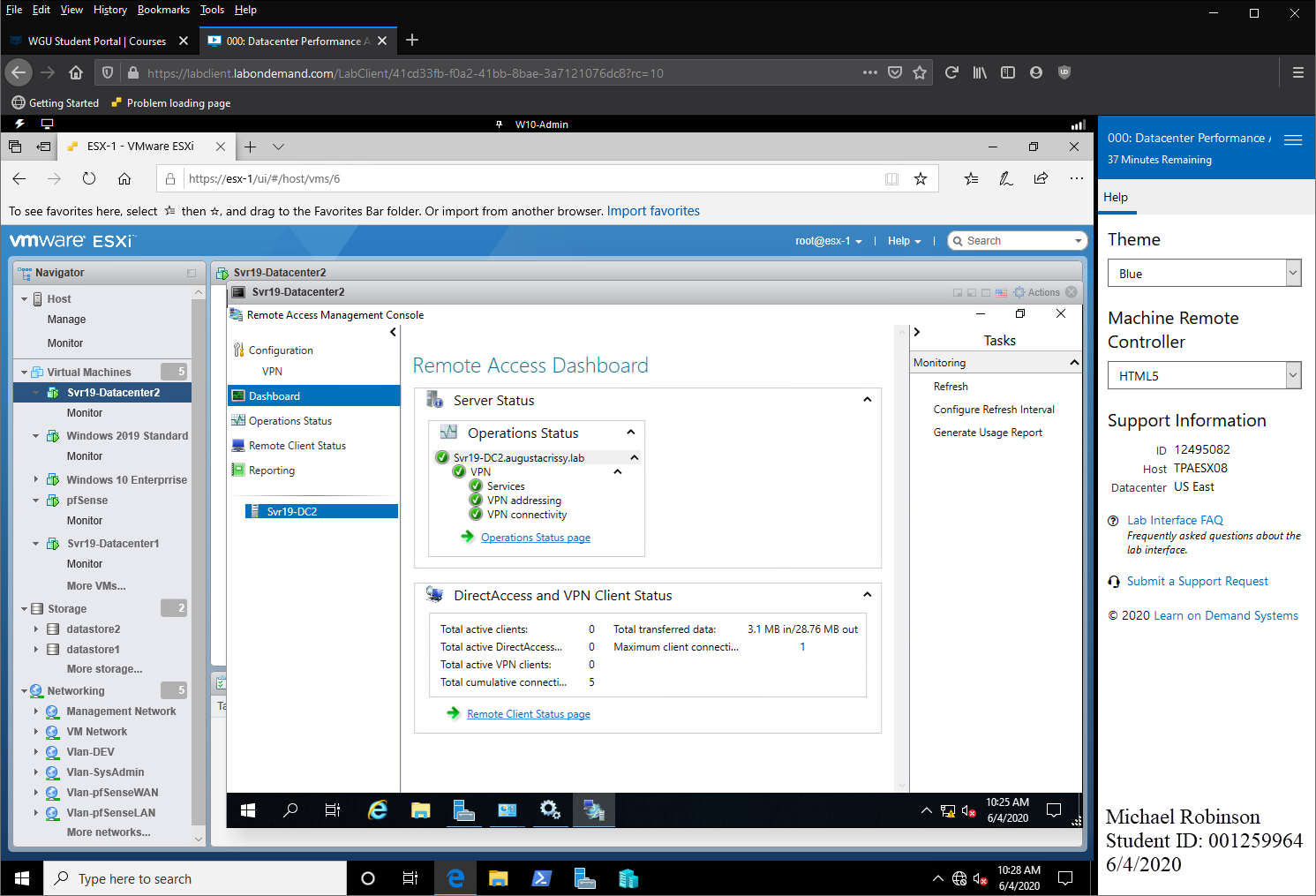
# Phase 3 - Active Directory, Remote Access and verified are functional



This screenshot shows the Active Directory deployed on the Windows 2019 Standard server that was utilized for the AD Domain.

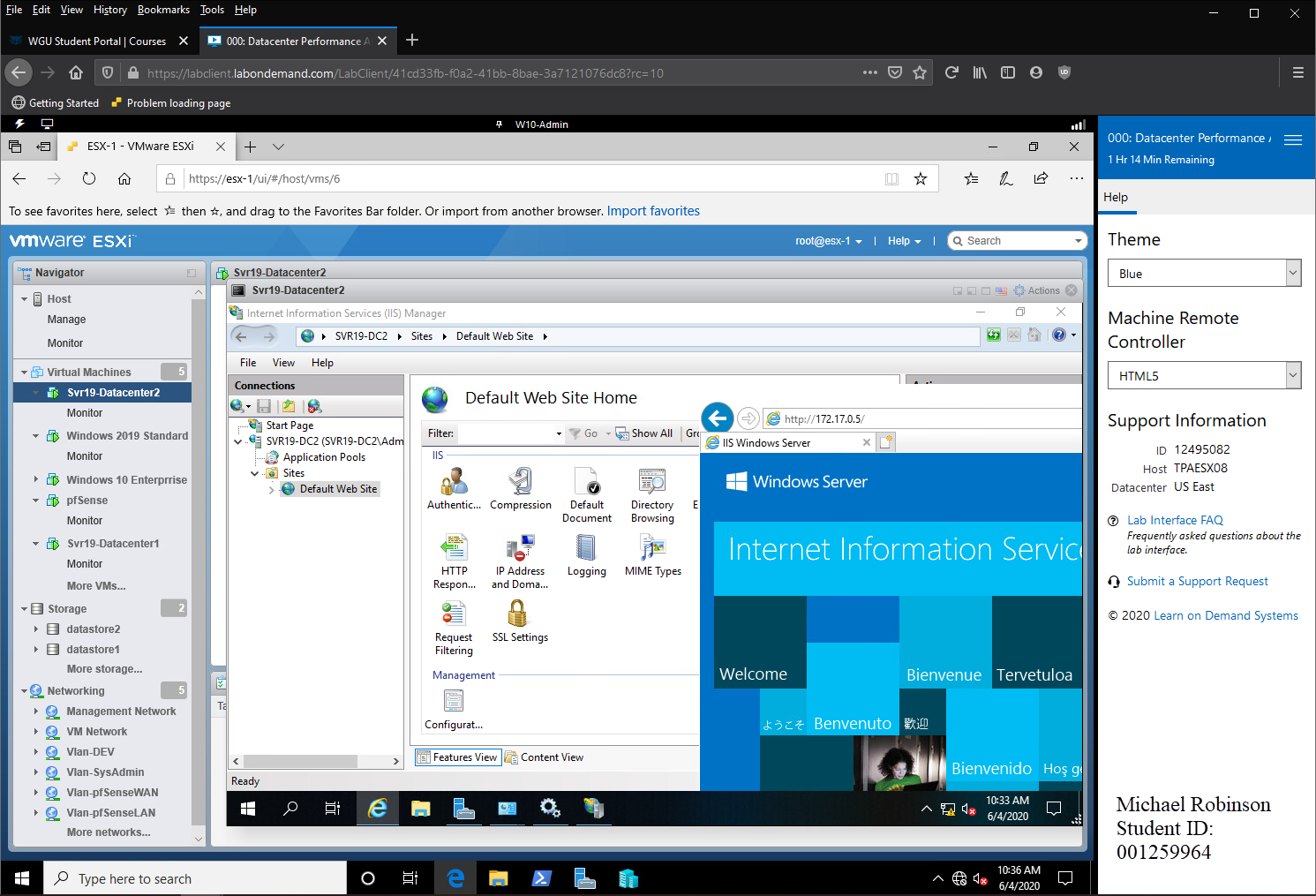


This screenshot reflect the VPN RAS services deployed to Srv19-Datacenter1.

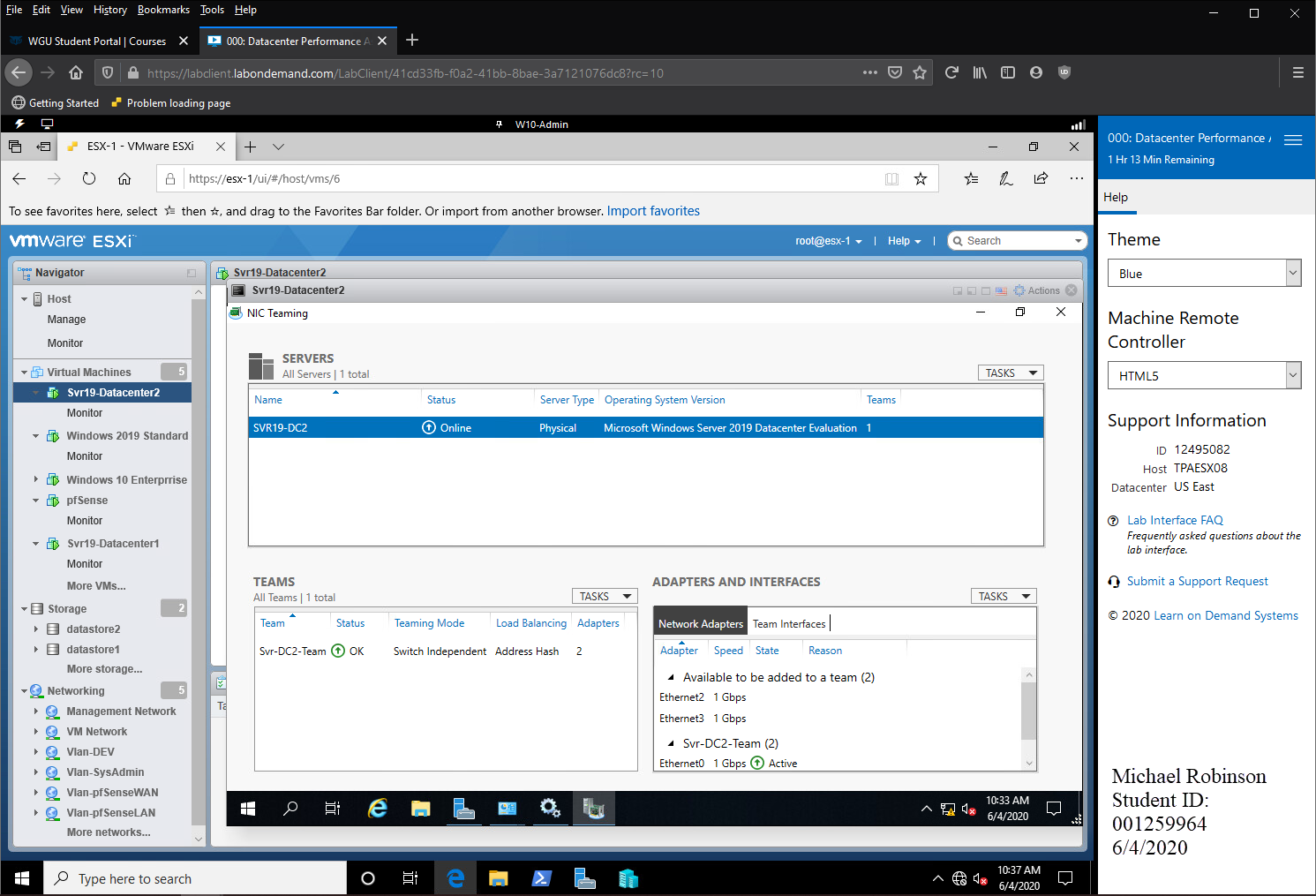


This screenshot reflect the VPN RAS services deployed to Srv19-Datacenter2.

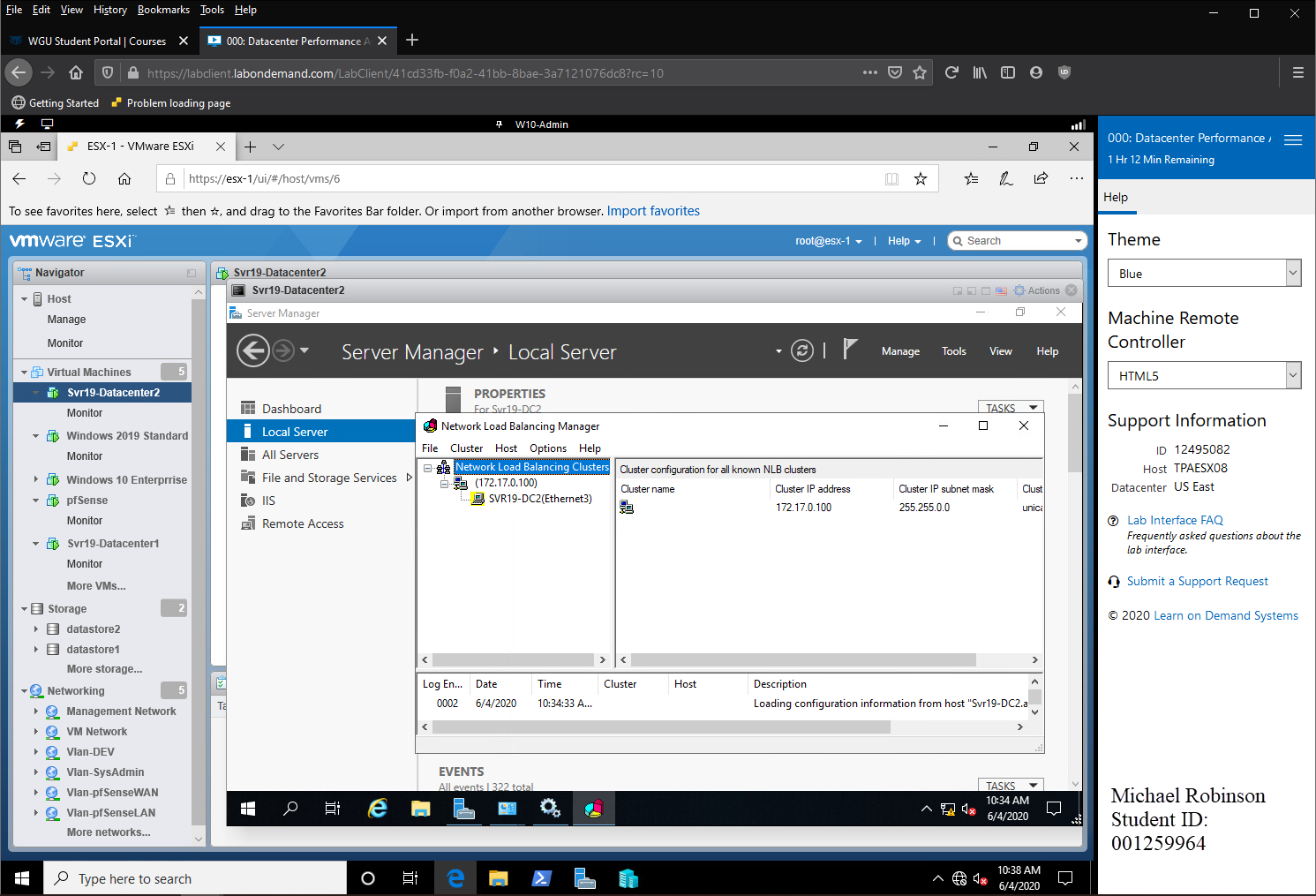
# phase 4 - Deploy IIS Datacenter Servers, Team NICS and Load Balance



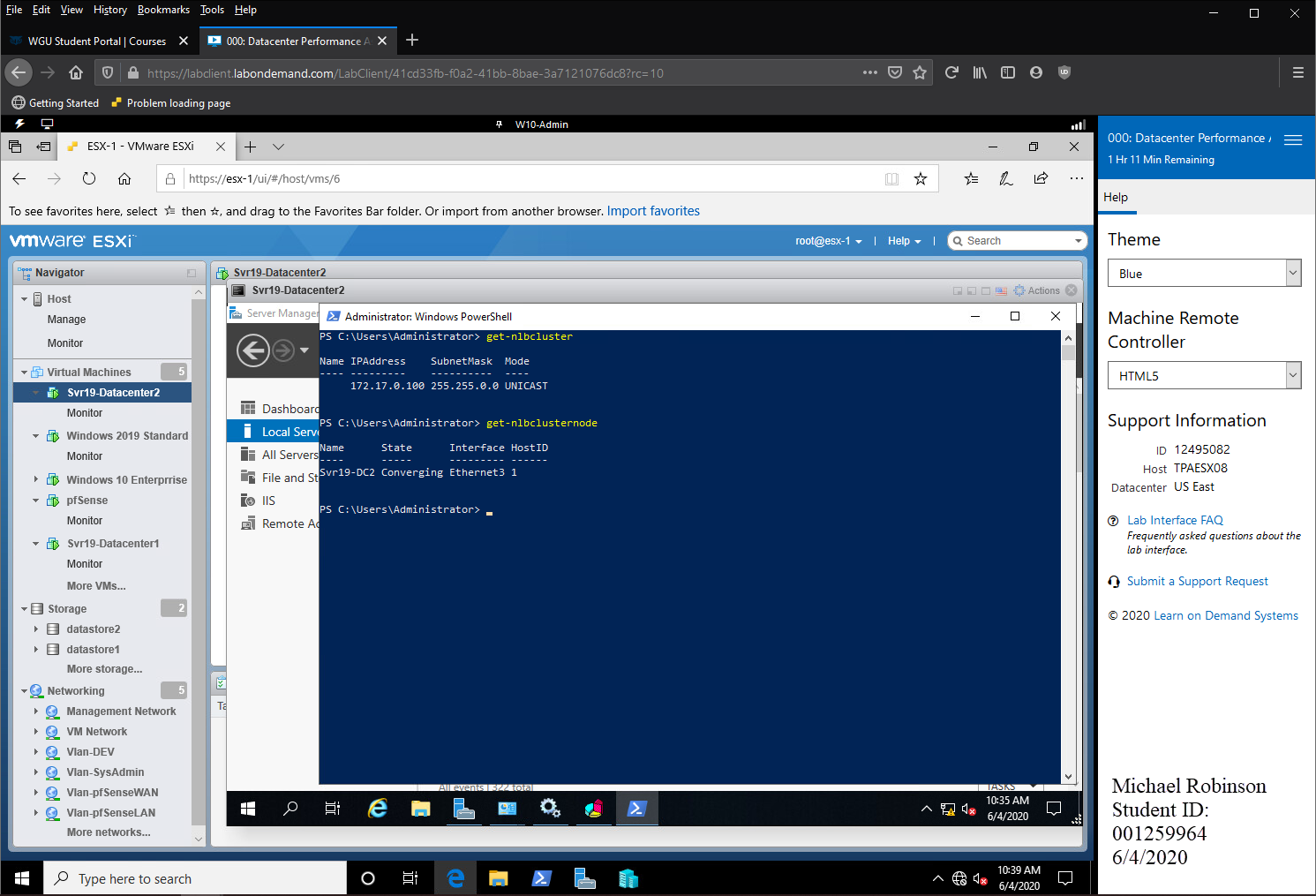
This screenshot reflects the IIS webserver deployed to Srv19-Datacenter2 running and operational.



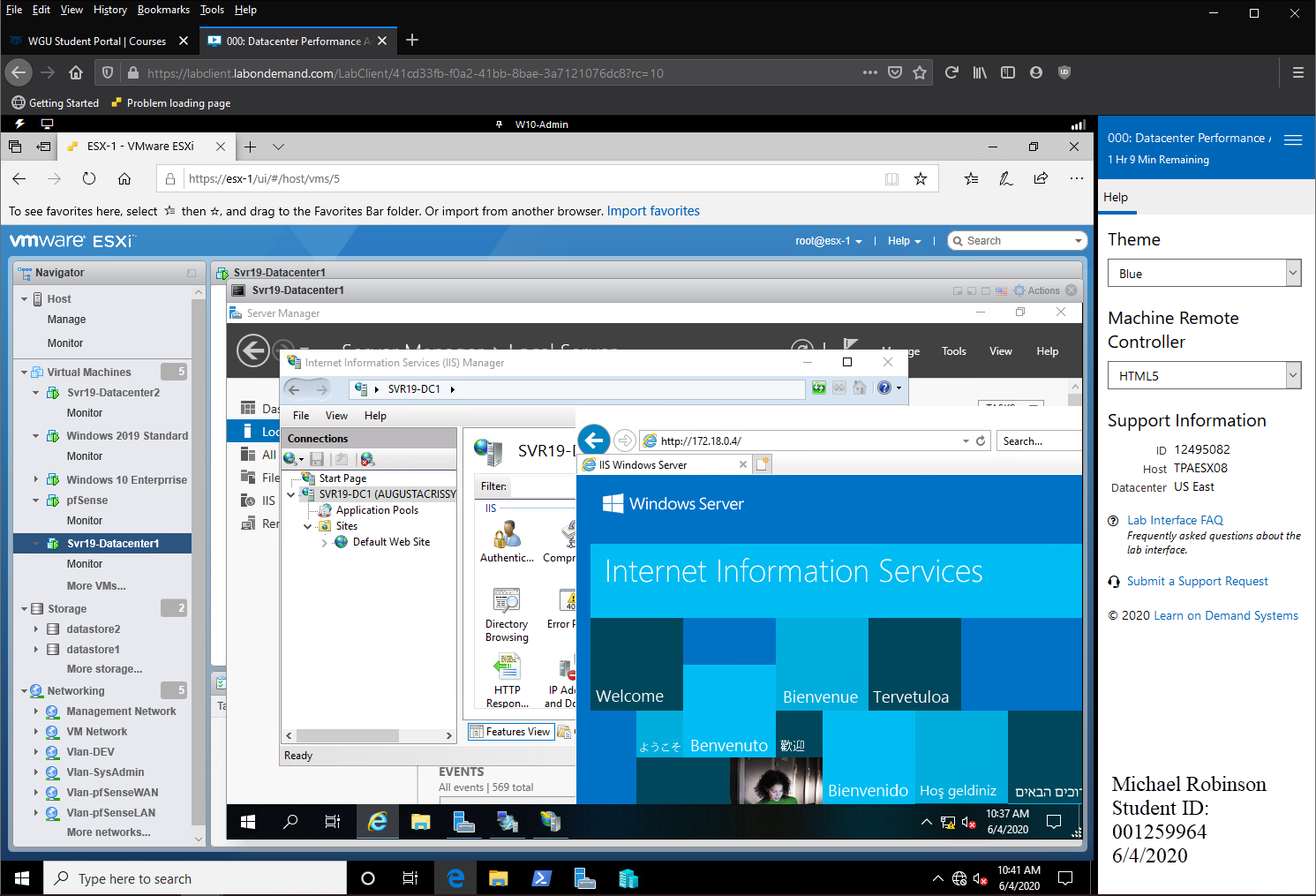
This screenshot reflects the NIC Teaming on Srv19-Datacenter2 running and operational.



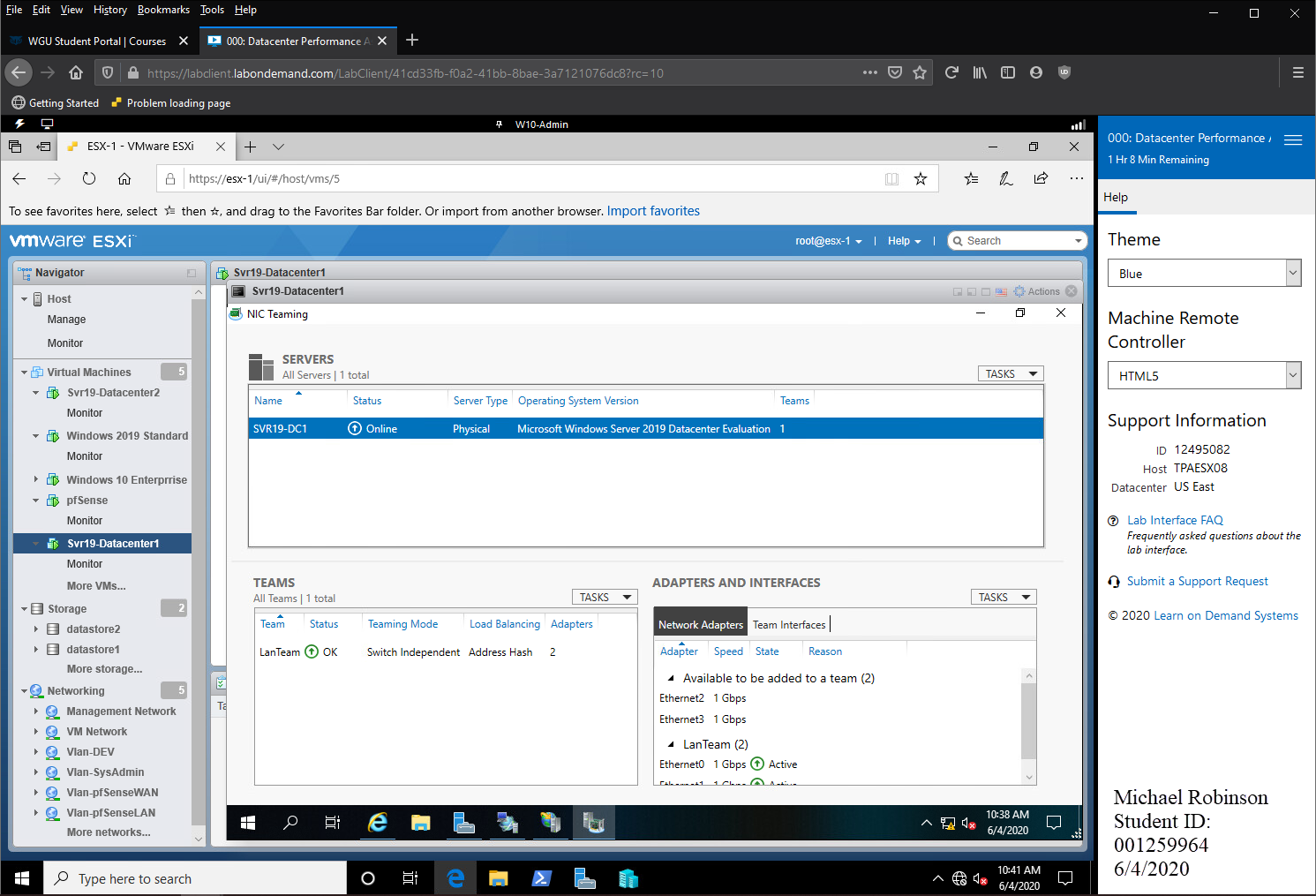
This screenshot reflects the Network Load Balancing deployed to Srv19-Datacenter2 running and operational on IP 172.17.0.100.



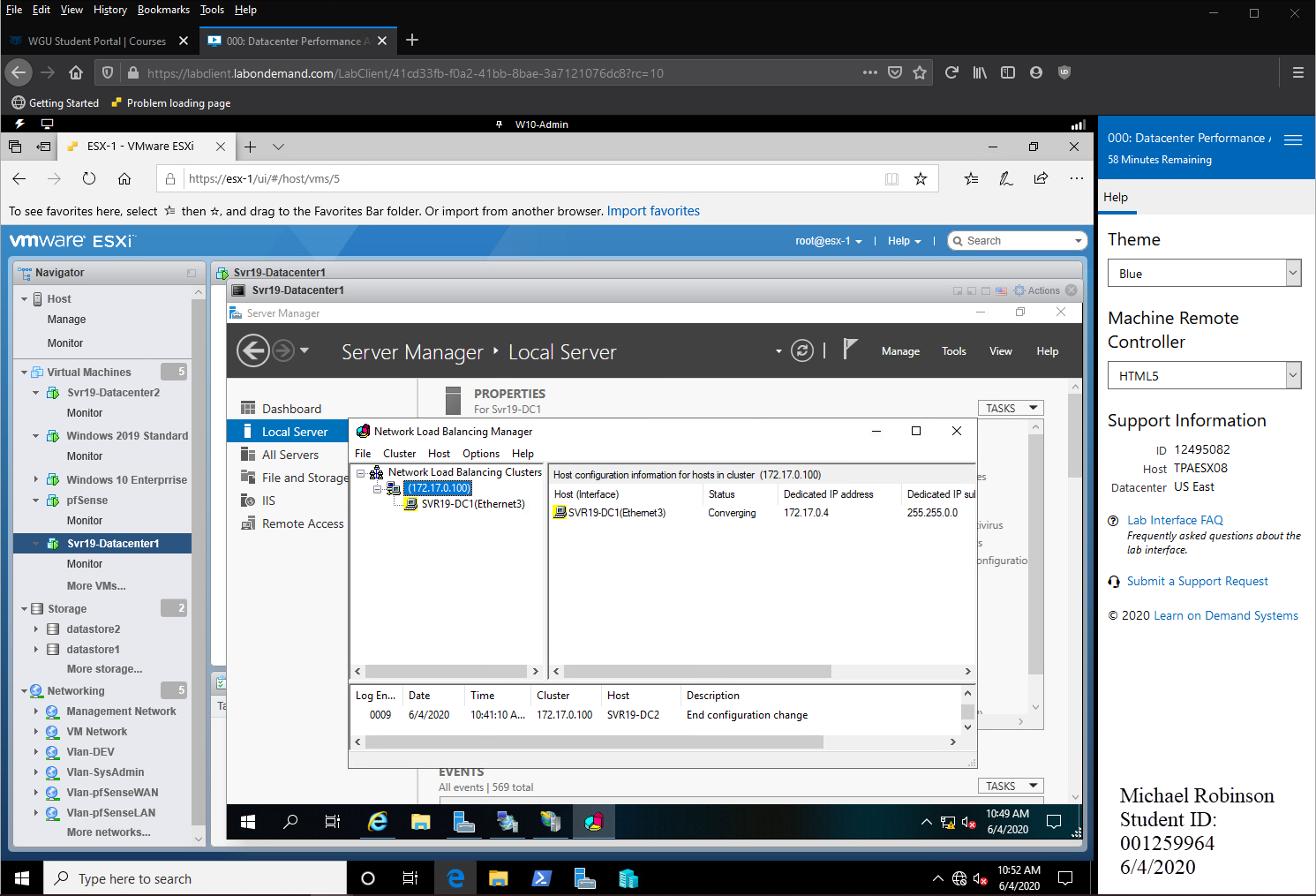
This screenshot reflects the Network Load Balancing deployed to Srv19-Datacenter2 running and operational on IP 172.17.0.100 NLBCluster and NLBClusterNode.



This screenshot reflects the IIS webserver deployed to Srv19-Datacenter1 running and operational



This screenshot reflects the NIC Teaming on Srv19-Datacenter1 running and operational.

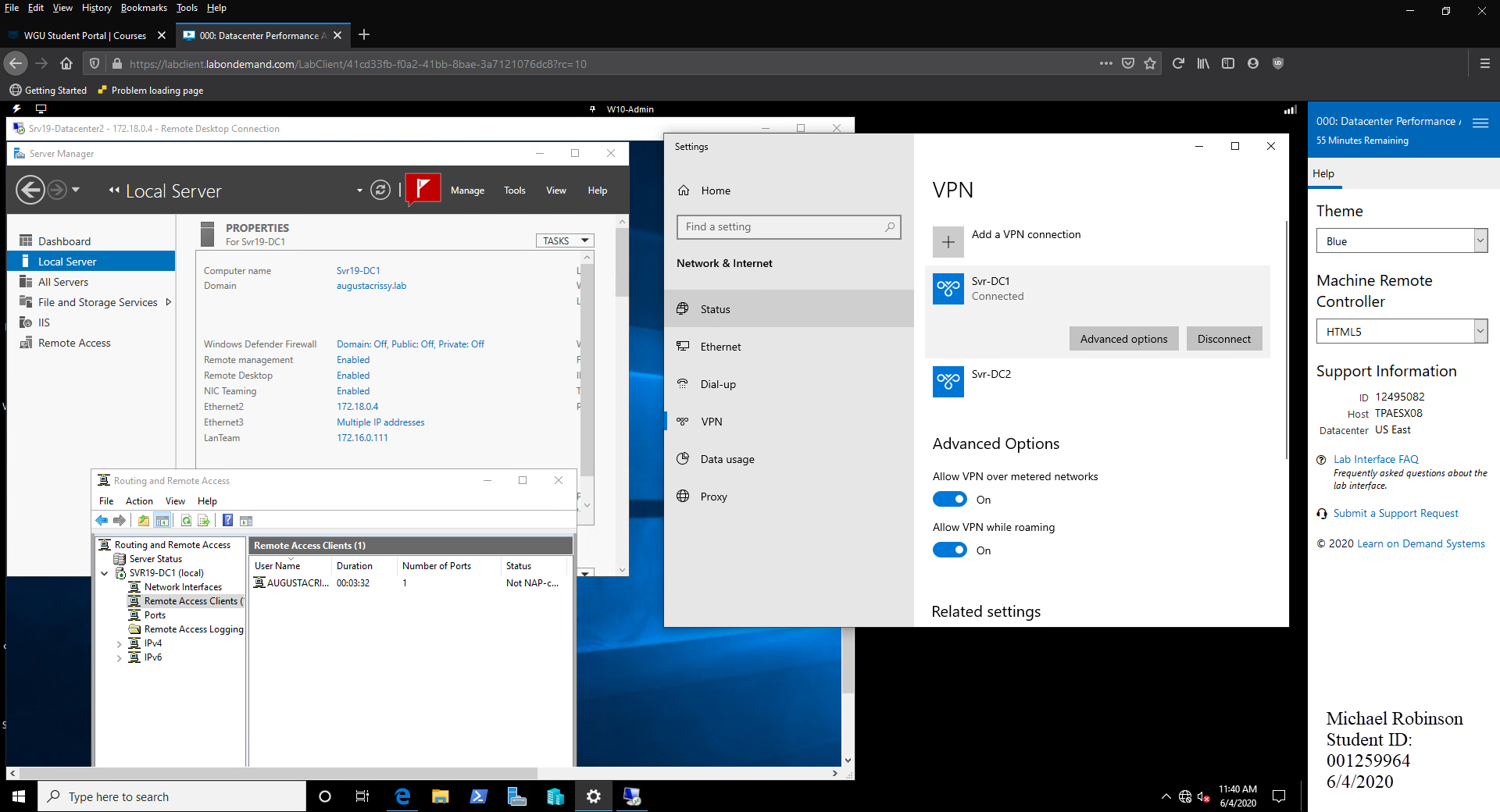


This screenshot reflects the Network Load Balancing deployed to Srv19-Datacenter1 running and operational on IP 172.17.0.100 NLBCluster and NLBClusterNode.

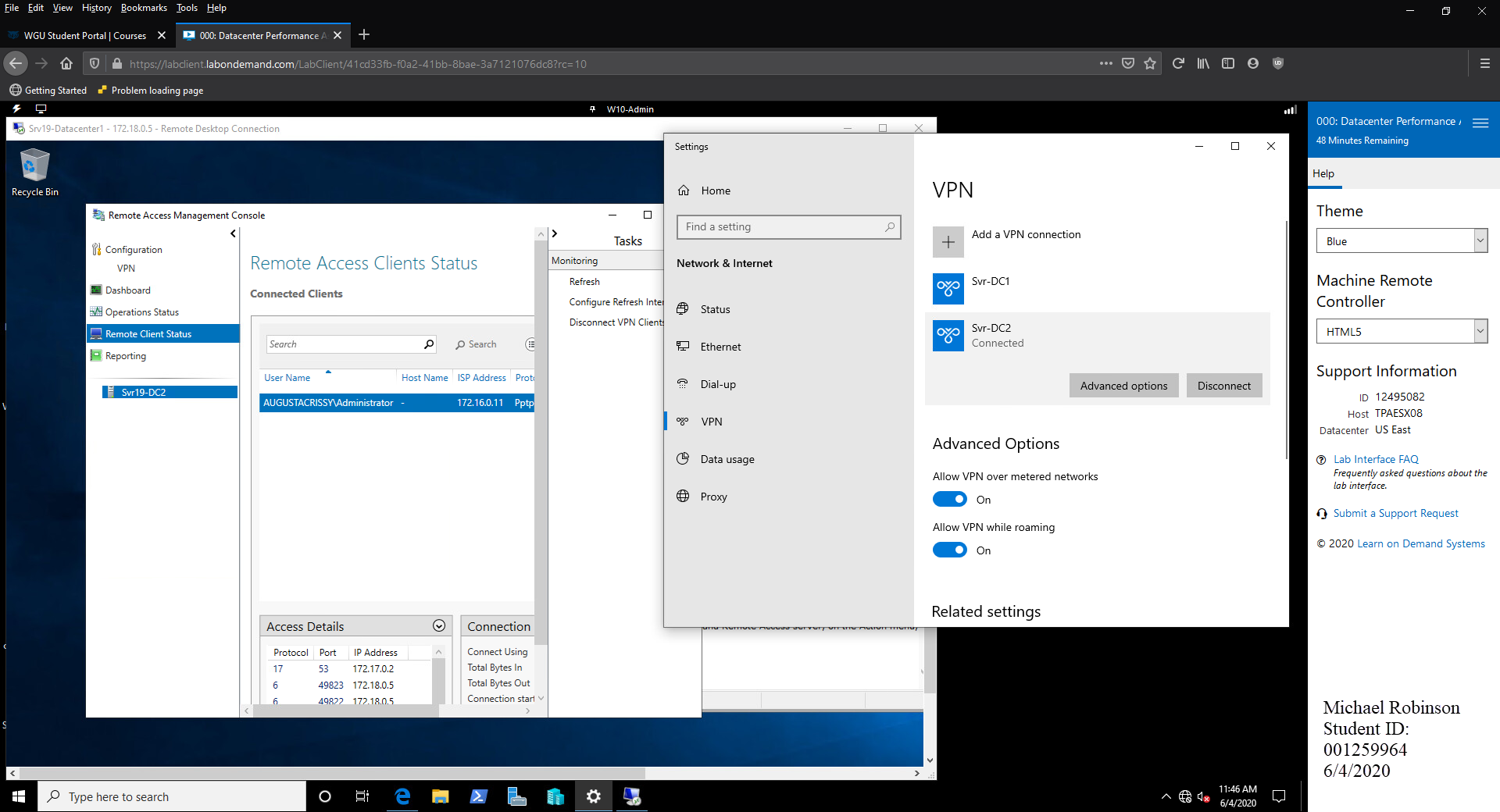


This screenshot reflects the Network Load Balancing deployed to Srv19-Datacenter1 running and operational on IP 172.17.0.100 NLBCluster and NLBClusterNode

# phase 5 - Validate VPN, RDP Externally



This screenshot reflects the VPN Operational into Srv19-DC1 and access to RDP to the Server.



This screenshot reflects the VPN Operational into Srv19-DC2 and access to RDP to the Server.