Jeys Consulting Group

Proof-of-Concept Design

D087- Data Center Virtualization

Chris Jeys

8-26-2022

WESTERN GOVERNORS UNIVERSITY

CONTENTS

A. SYSTEMS ANALYSIS OF CURRENT ENVIRONMENT

Augusta Crissy Detective Games have become increasingly popular with the widespread adoption of virtual reality technology. The supporting infrastructure will need to be updated to accommodate this growing demand. There are several options available to increase data center capacity. This proof of concept is focused on a hybrid-cloud local data center solution.

One such justification for implementing a hybrid-cloud solution is the ability to increase server space and capacity without incurring the costs of adding data centers. Typically, the deployment of physical servers, storage, requires datacenter floorspace which can incur tremendous costs and takes a long time to scale when needed. With the use of virtualization, these issues with a typical on-prem datacenter environment are easily overcome.

There are more justifications for implementing this hybrid-cloud solution than just saving on real estate that more datacenters will require. Additional costs will be saved by virtualizing the underlying hardware like routers, switches, and servers. One server built with the correct resources and properly configured can be utilized to create many virtualized components that previously would have been built on physical hardware. This helps to reduce the overall footprint of the supporting infrastructure.

The last benefit and justification for this solution is the speed of deployment achieved with this hybrid-cloud implementation. In the current configuration, all hardware components will need to be researched, purchased, prepped, and deployed. These steps require additional manpower, knowledge, and skills to deploy changes to the data center environment. Speed of deployment to support the growing subscriber base can easily be achieved by taking advantage of virtualization technology. New virtual servers, and the supporting infrastructure components, can be spun up and added to the existing domain within days or weeks rather than months saving on manpower in the process.

B. VIRTUALIZATION SOLUTION

HOW THE SOLUTION MEETS BUSINESS NEEDS

For the proposed hybrid-cloud solution, a virtualized environment will be deployed to an ESXi host, proving the value and merit of utilizing virtualization technology. To fully productionalize this solution, vSphere Datacenter should be used to take advantage of active directory integration and more robust features that are not available in the free ESXi release.

HOW THE SOLUTION MEETS THE TECHNICAL REQUIREMENTS

The proposed solution has been deployed with several virtualized components that satisfy the requirements laid out for this proof of concept. Specific details for the virtualization technology presented in this solution are listed below.

VIRTUAL HOSTS

The following hosts/virtual machines will be deployed as part of the hybrid-cloud solution:

DC01 (Windows Server 2019)

This virtual machine will be the Domain Controller for *augustacrissy.lab* and provide DNS services to the other virtual machines in this solution. In addition, DC01 is configured with DCHP to issue IP addresses for the DEV network. Windows Server 2019 is the underlying operating system used for this virtual machine.

Router (pfSense)

This virtual router is configured as the remote access endpoint to the network. In addition, it also serves as the primary network and main gateway for this virtualized solution.

IIS01 & IIS02 (Windows Server 2019 Datacenter)

These virtual machines are configured with IIS Webserver and Remote Access Server. Network Load Balancing is also configured in conjunction with NIC Teaming. This will provide redundancy at the server level by balancing web requests between them and at the NIC level.

JMP01 (Windows 10 Enterprise)

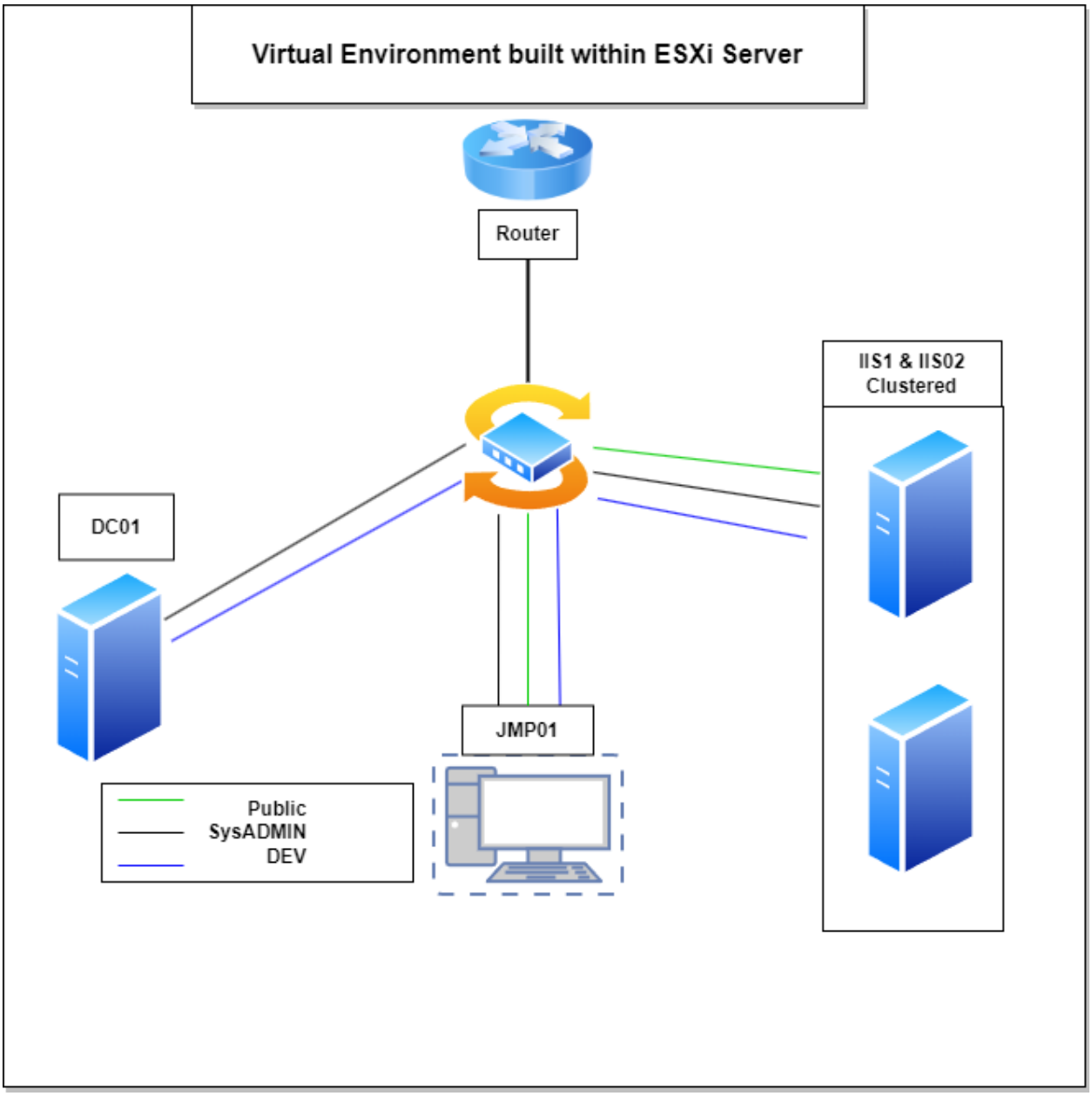
This virtual machine serves as the gateway host for remote access, via RDP, to internal services and virtual machines.

NETWORKING

Virtual switches, one per subnet, and port groups are deployed to isolate traffic between the different networks. A single virtual switch could also be utilized. However, this solution takes advantage of the low costs and quick deployment of virtualization technology by implementing multiple virtual switches to easily segregate traffic for admin and troubleshooting purposes.

Host	Interface	IP	VLAN	vSwitch
Router (pfSense)	Em0	172.16.0.111/24	Public	vSwitch
	Em1	192.168.1.1/24	SysADMIN	SysADMIN
	Em2	10.0.6.111/24	DEV	DEV
ESXi Server Host		172.16.0.213		
DC01 (Svr-19-Stanard)	Eth0	192.168.1.102/24	DEV	DEV
	Eth1	10.0.6.12/24	SysADMIN	SysADMIN
IIS01 (Srv-Datacenter1)	Eth0	172.16.0.108/24	Public	vSwitch
	Eth1	172.16.0.107/24	Public	vSwitch
	Eth2	10.0.6.11/24	SysADMIN	SysADMIN
	Eth3	192.168.1.101/24	DEV	DEV
IIS02 (Srv-Datacenter2)	Eth0	172.16.0.110/24	Public	vSwitch
	Eth1	172.16.0.109/24	Public	vSwitch
	Eth2	10.0.6.8/24	SysADMIN	SysADMIN

	Eth3	192.168.1.100/24	DEV	DEV
IIS01 & IIS02 Load Balancer		172.16.0.225		
JMP01 (Win10-Ent)	Eth0	172.16.0.106/24	Public	vSwitch
	Eth1	DHCP assigned thru DC01	DEV	DEV
	Eth2	10.0.6.7/24	SysADMIN	SysADMIN



C. SECURITY

The following security measures will be taken to protect the network and data within this hybrid-cloud solution.

C.1. VIRUS SCAN SYSTEM

Windows Defender will serve as the default antivirus solution. It has the capability to push and deploy virus definitions to the virtual machines along with the configuration of alerts for when unusual activity and threats are detected within the environment. If there are other requirements due to governmental regulations or other commercial purposes, a more robust antivirus solution can be implemented.

C.2. FIREWALL RULES

For all Windows operating systems, firewall rules will be implemented and enforced with Active Directory. All inbound entry points will follow the principles of 'least privilege' to further enhance the security implementation. To reduce managerial overhead, a stateful firewall should be the primary choice to minimize the number of outbound rules. In addition, configuration management should be automated to secure network-level controls in a standard and uniform manner. This will also help simplify admin and auditing of all firewall-related activities.

Virtual Machines	DC01	IIS01 & IIS02
Inbound Rules (Port)	Permit HTTP (80), HTTPS (443), DNS (53), RDP (3389), & DHCP (67)	Permit HTTP (80), HTTPS (443), & RDP (3389)
Outbound Rules	Permit All	Permit All

C.3. ACCESS CONTROL LISTS

Access control lists, similar to the firewall rules, will follow 'least privilege' principles to ensure that access is allowed on an "as needed" basis. Login credentials for admin, and other users, will be kept separate so that the supporting infrastructure can be managed while also being utilized by the subscriber base without them interfering with each other. With the virtual machines being joined to the augustacrissy.lab domain, more granular control over the resources and supporting infrastructure can be achieved.

The Network Access Control List will be applied to the VLANs as follows:

DC01	VLAN-DEV: Access to IIS01, IIS02, & JMP01 VLAN-SysADMIN: Access to IIS01, IIS02, & JMP01
JMP01	VLAN-DEV: Access to IIS01 & IIS02 VLAN-SysADMIN: Access to DC01, IIS01, & IIS02 VLAN-Public: Access to IIS01 & IIS02
IIS01 & IIS02	VLAN-DEV: Access to DC01 & JMP01 VLAN-SysADMIN: Access to DC01 & JMP01 VLAN-Public: Access to JMP01

C.4. SECURITY GROUPS

Windows Security Groups is another security feature that will be used to help follow the principle of 'least privilege.' This will allow for the separation of rights and permissions to perform tasks by providing manageable groups where these can be configured, tracked, and audited. Entry into the various security groups will follow the appropriate approval process determined by Augusta Crissy Detective Games.

C.5. INFORMATION SECURITY MANAGEMENT

All applicable standards and procedures of ACDG will be followed to mitigate risks and help with compliance management. In addition, IOS-IEC 27001 standards for Information Security Management Systems will also be followed to capture, review, and build upon the current InfoSec policies and procedures.

D. IMPLEMENTATION PROCESS

The following chart lists the phases, milestones, and dependencies for this hybrid-cloud solution.

Phase	Milestone	Dependencies
Build	Virtual machines deployed	The virtual machines will be built, set up, & deployed for the separate operating systems required for this implementation.
Network	Network infrastructure deployed, configured & secured	The network will be mapped out, virtual switches & port groups set up, virtual machine IP addresses configured & 'teamed' where required, & firewall rules put in place.
Services & Roles	Configure services & assign user roles	The virtual machines will have DNS, DHCP, remote desktop services, network load balancing, & IIS enabled based on the configuration requirements.
Test & Validate	Verify functionality of the implementation	Benchmark testing will be performed by the user base to ensure the new virtualized solution meets the performance and functionality requirements while also providing them the opportunity to give feedback.

E. PERFORMANCE TUNING

For this hybrid-cloud solution, NIC teaming will be implemented on the IIS01 & IIS02 servers. Network Load Balancing will also be utilized on the network. With the increased amount of network adapters attached to each server along with NLB, network throughput will be significantly increased while also providing redundancy at both the NIC and server levels.

Performance Monitor will also be used to capture and report on CPU utilization, network bandwidth, and memory consumption. This will help provide reports for a review of the environment to determine if there are opportunities to fine-tune or improve on the solution

ensuring all resources are correctly utilized without bottlenecks that will decrease the subscriber's gaming experience.

F. LOAD BALANCING

Load balancing will be implemented to provide ACDG's subscriber base with an improved gaming experience. This will help balance gaming traffic across the IIS01 & IIS02 servers to improve performance. This also provides the solution with redundancy in case of a server failure, as traffic can be redirected whenever a server goes offline unexpectedly.

TESTING STRATEGY

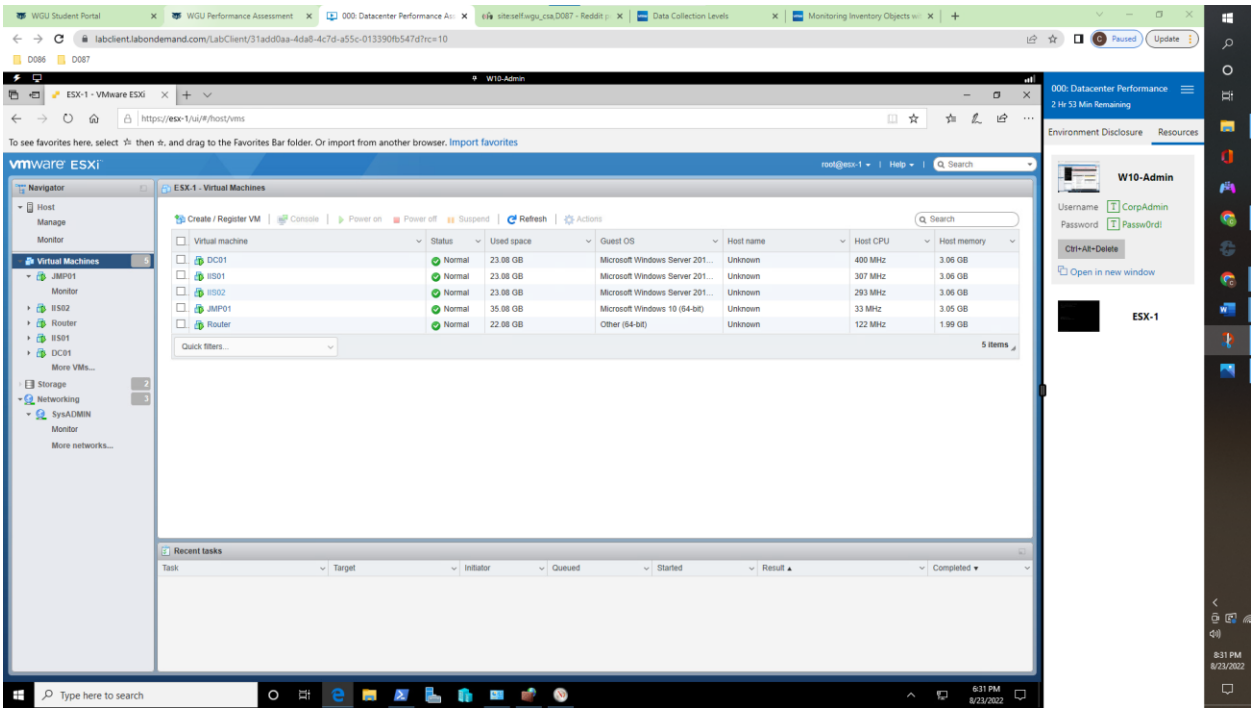
Test: This test will be performed with a group of users playing ACDG under normal circumstances. While users are in play, one of the virtual machines will be powered off to simulate a server failure or power outage.

Acceptance Criteria: With the load balancing strategy in place, users should be migrated to the online server automatically to prevent any issues and disruption to their gaming experience.

G. PROOF-OF-CONCEPT IMPLEMENTATION BUILD

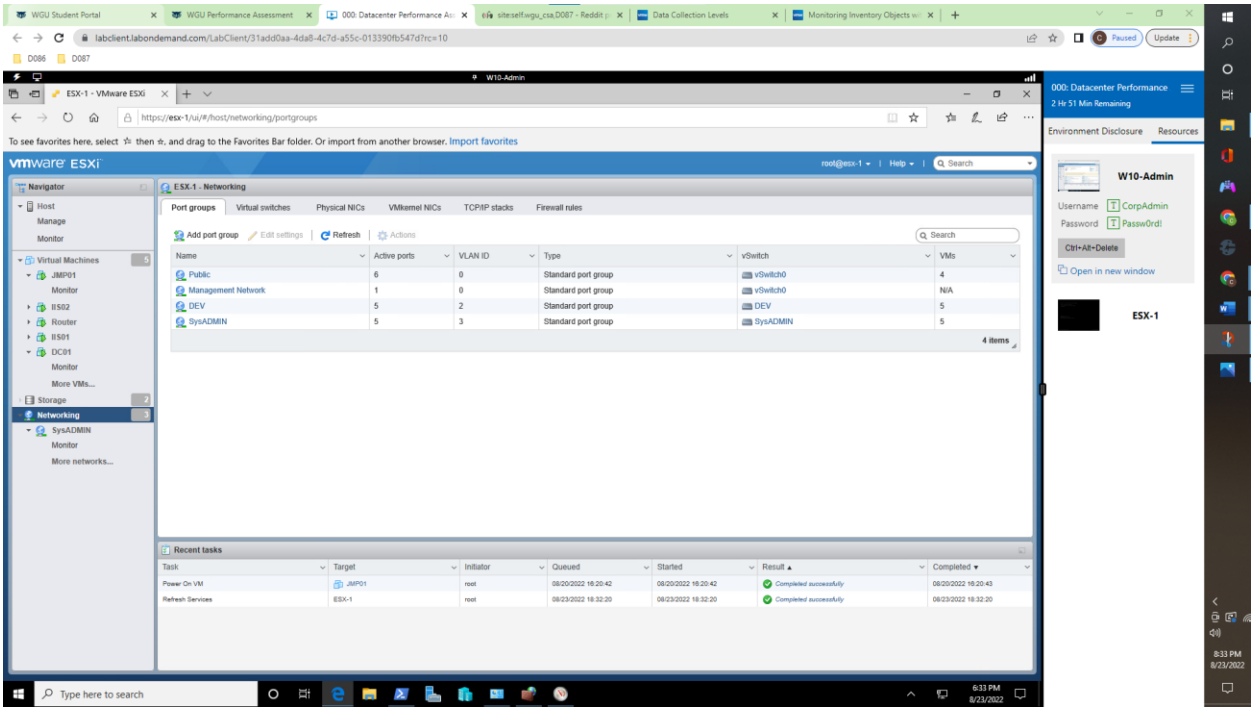
G.1. PHASE – BUILD

VMs: VMware ESXi with all VMs online

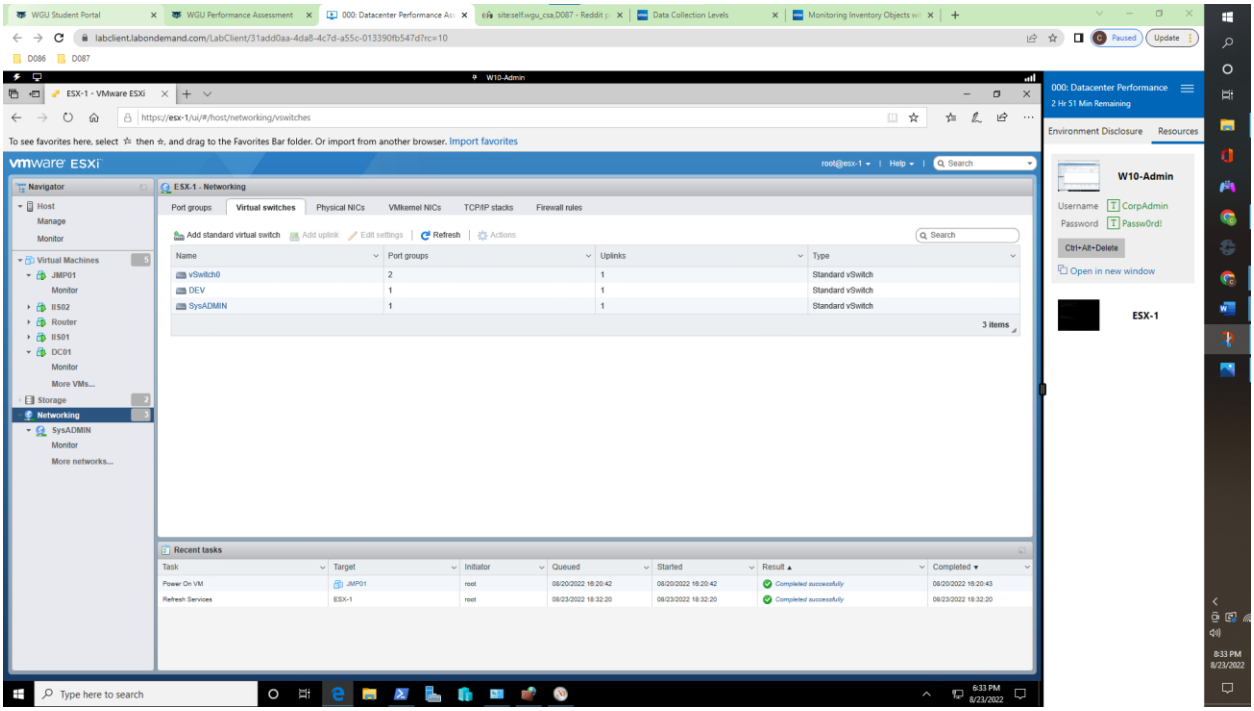


G.2. PHASE – NETWORK

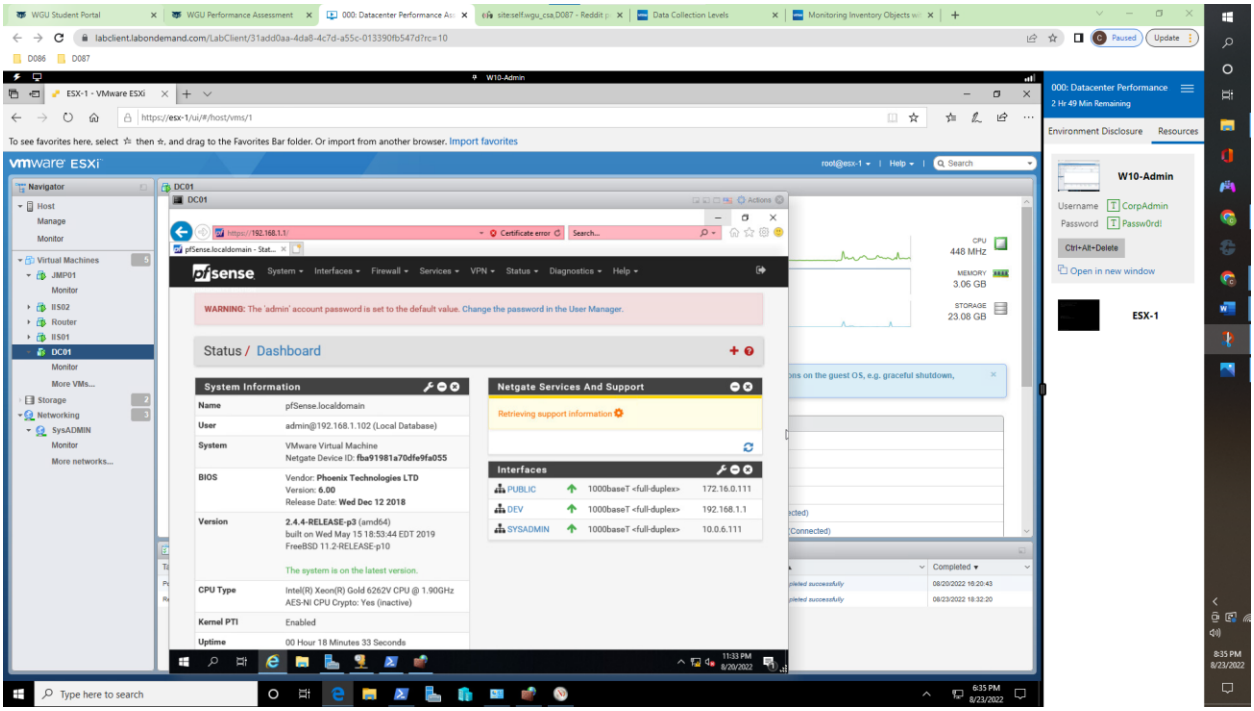
PORT GROUPS: Public, DEV, & SysADMIN port groups created



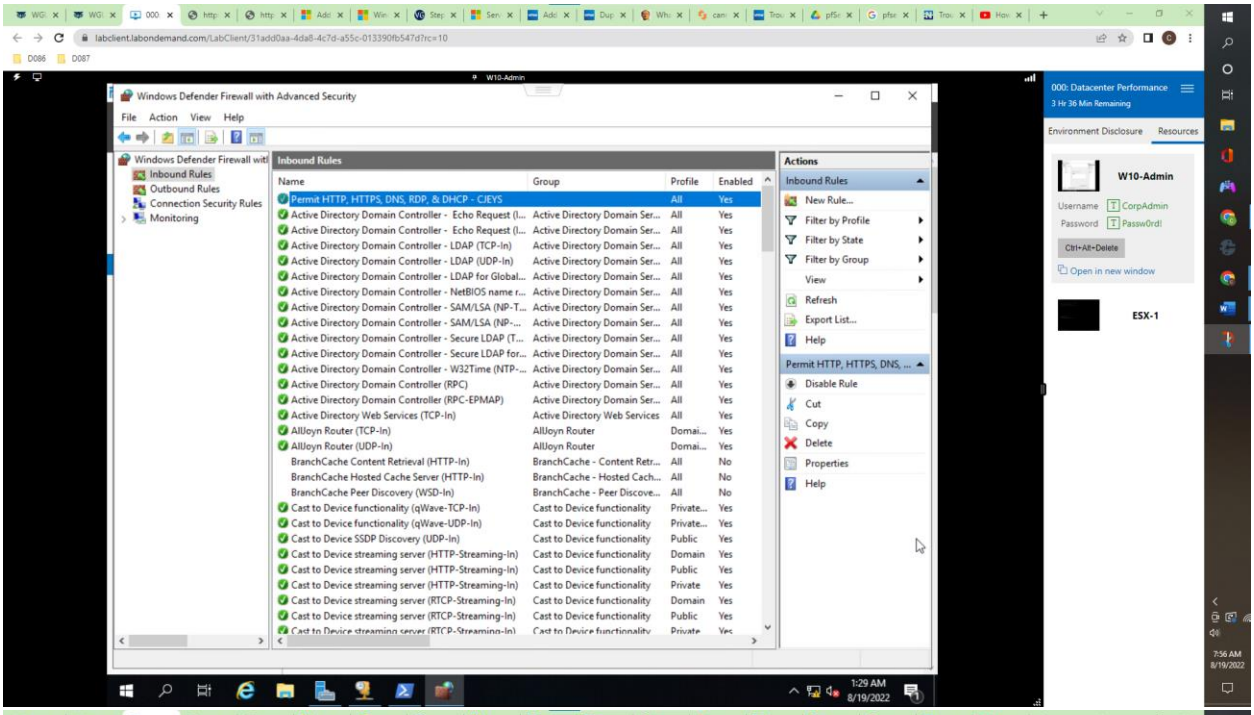
vSwitches: vSwitch0(Public), DEV, & SysADMIN virtual switches

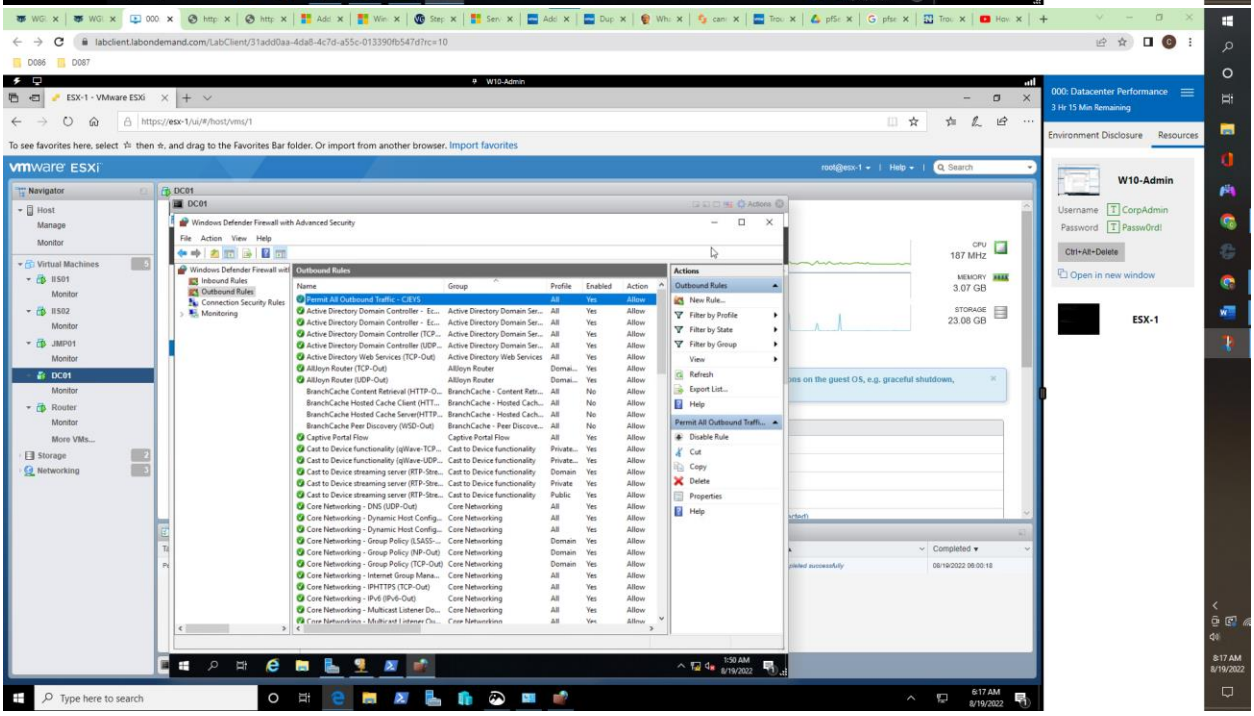


pfSense: Router online and configured

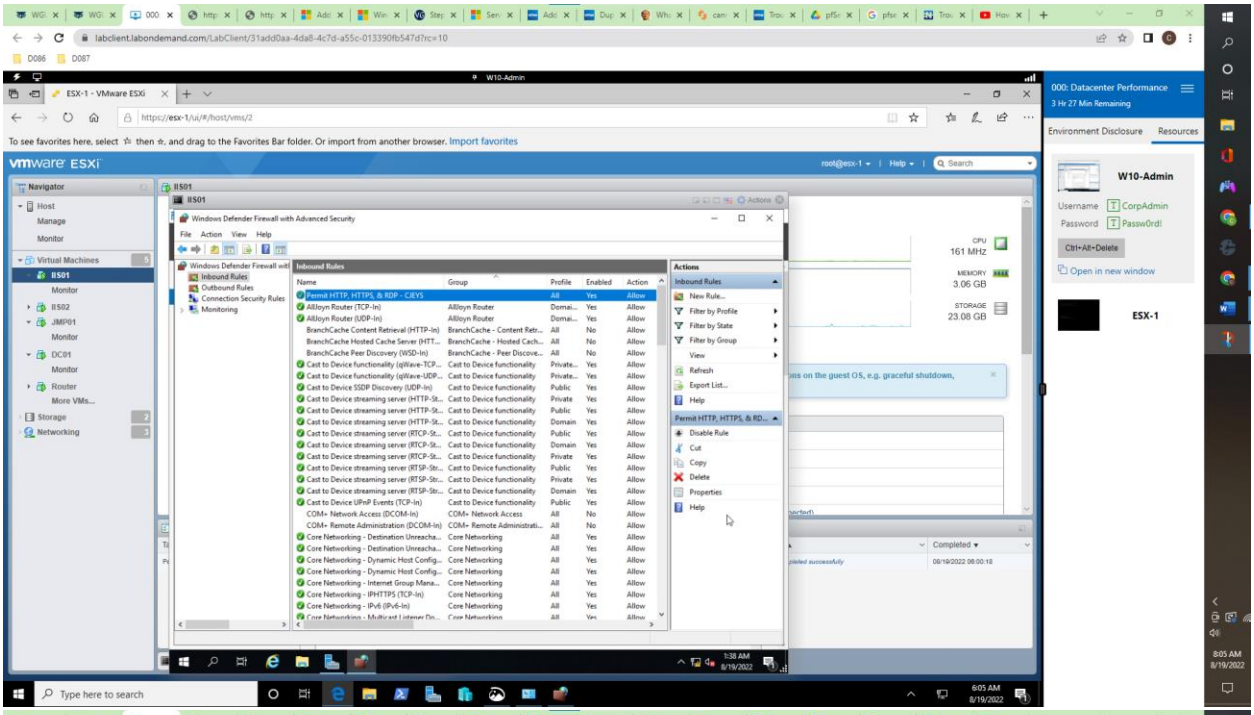


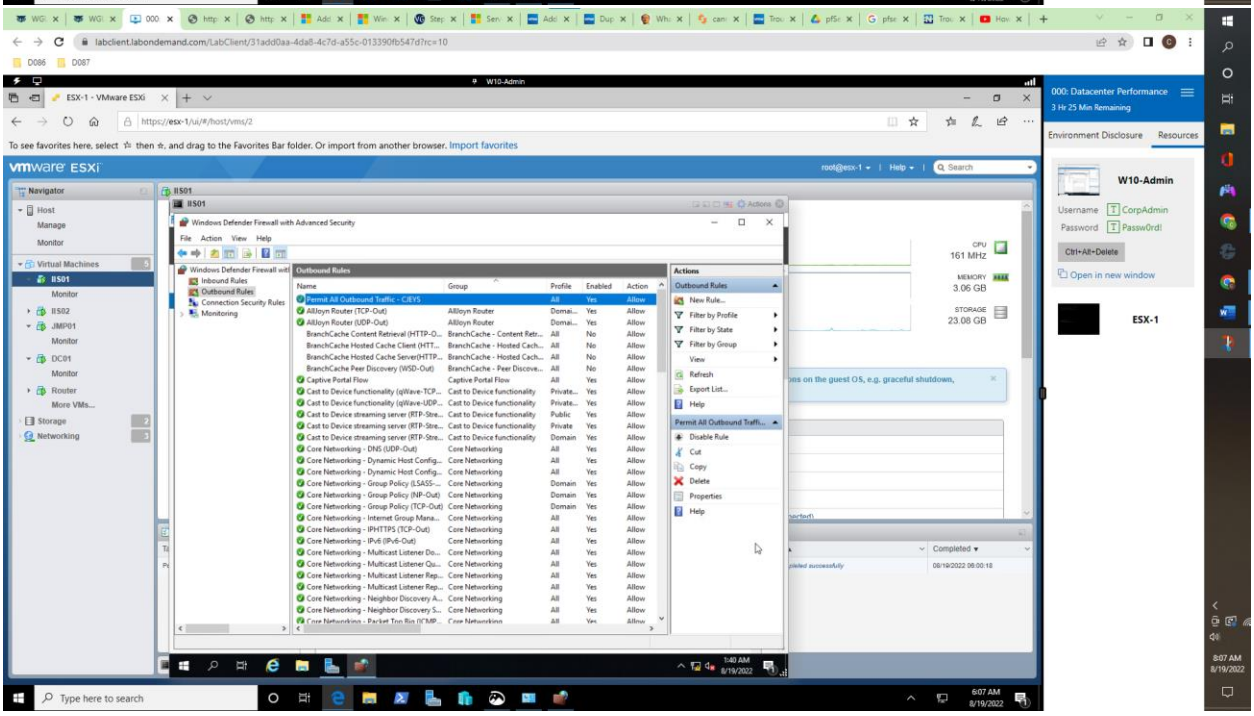
DC01: Firewall Inbound & Outbound rules enabled



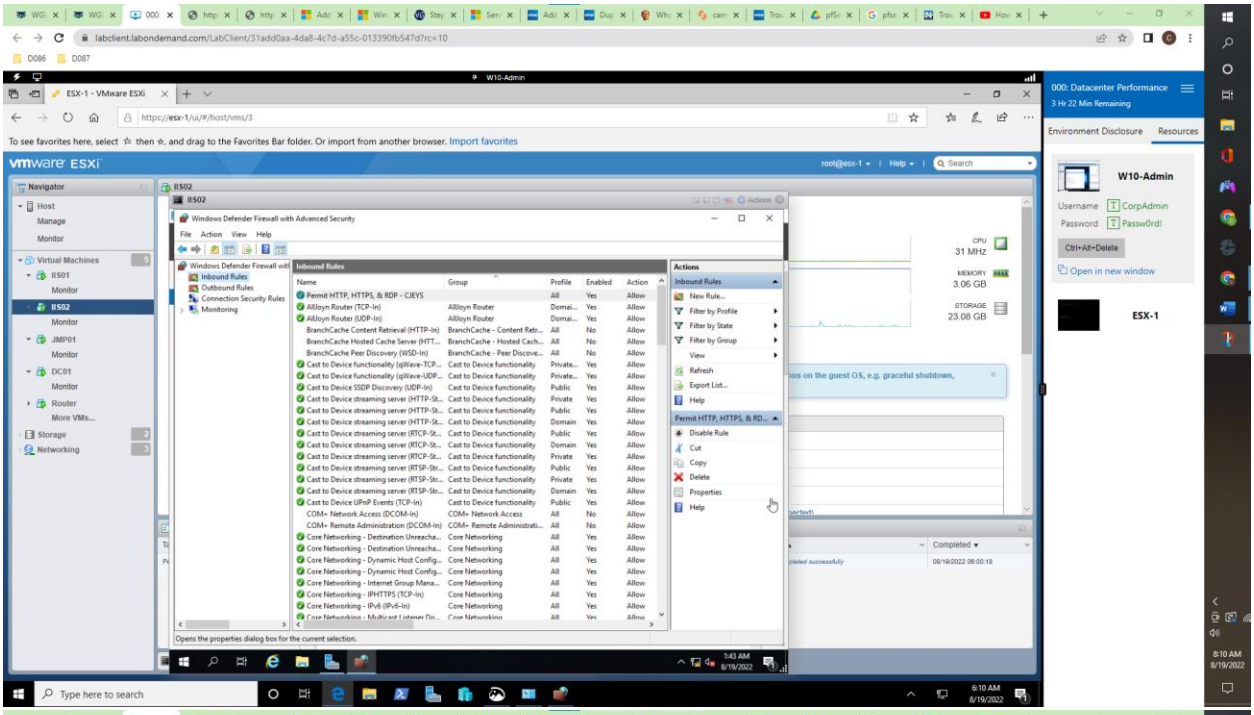


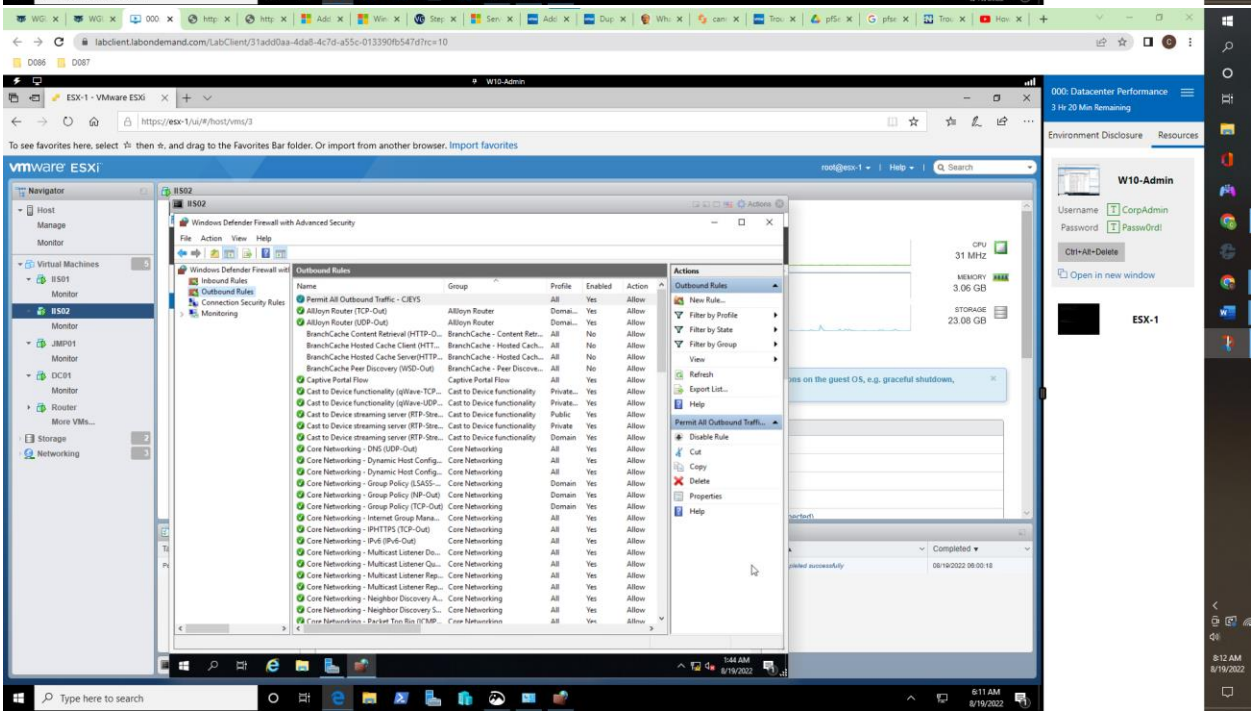
IIS01: Firewall Inbound & Outbound rules enabled





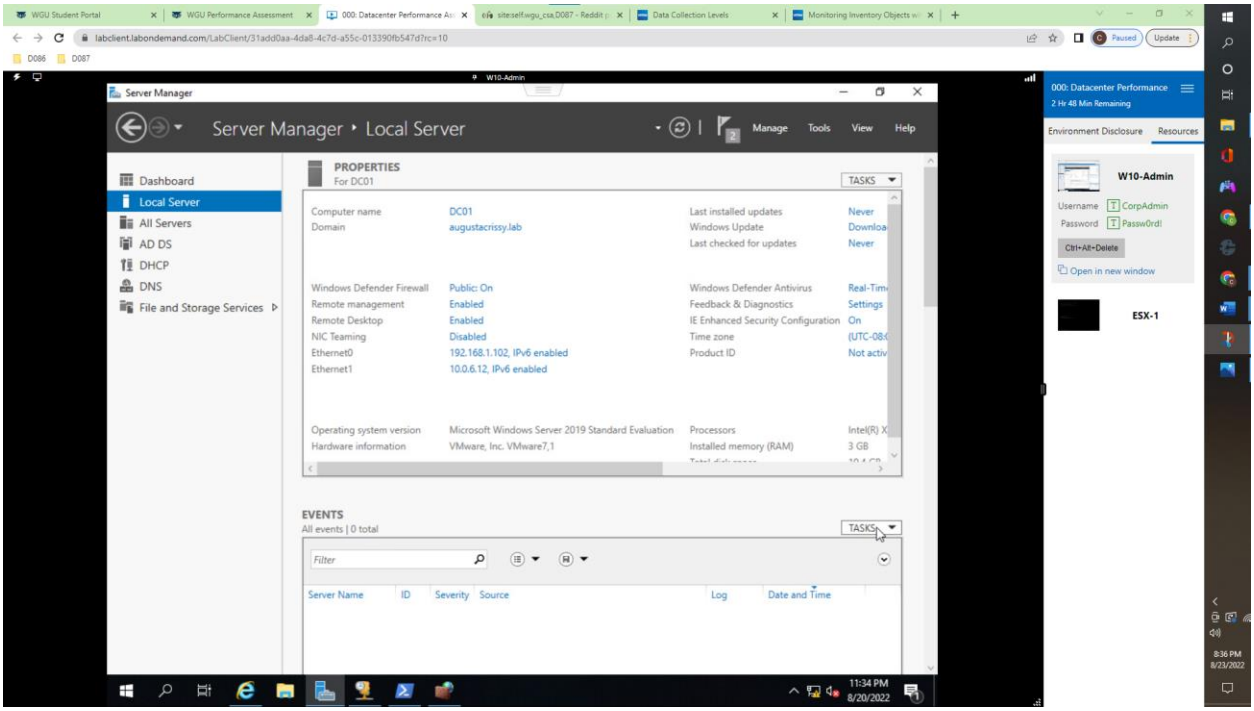
IIS02: Firewall Inbound & Outbound rules enabled



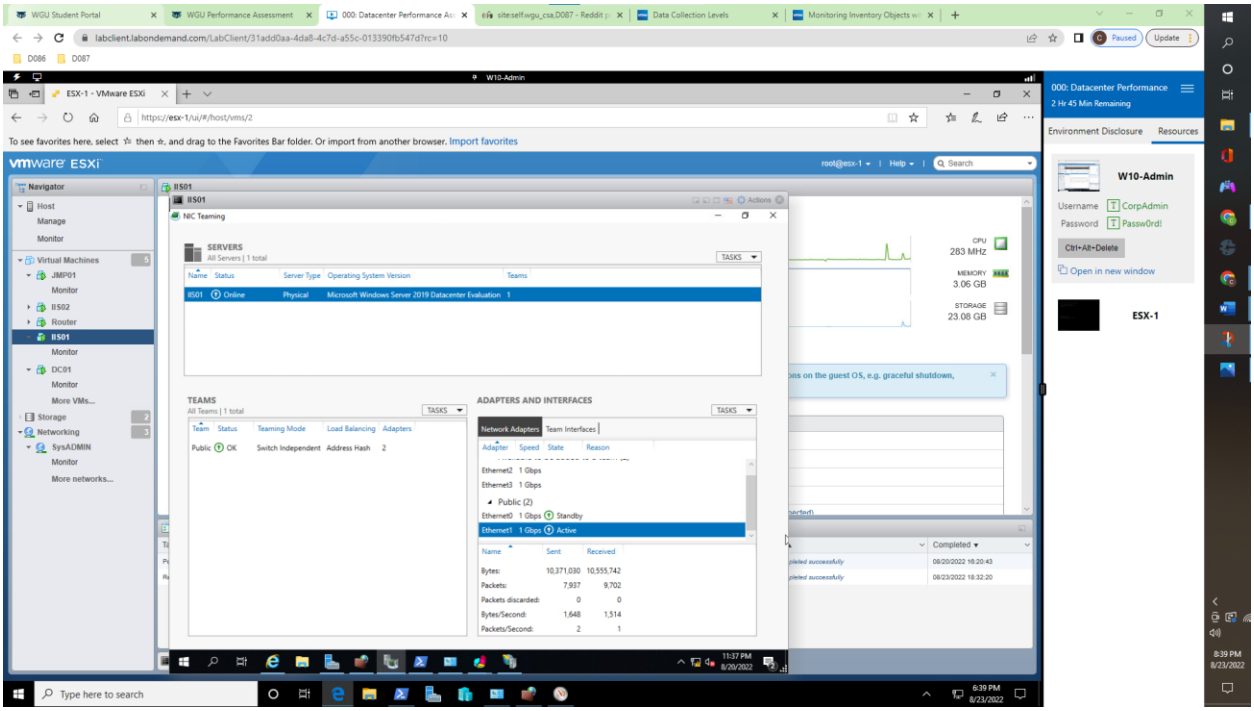


G.3. PHASE 3 – SERVICES & ROLES

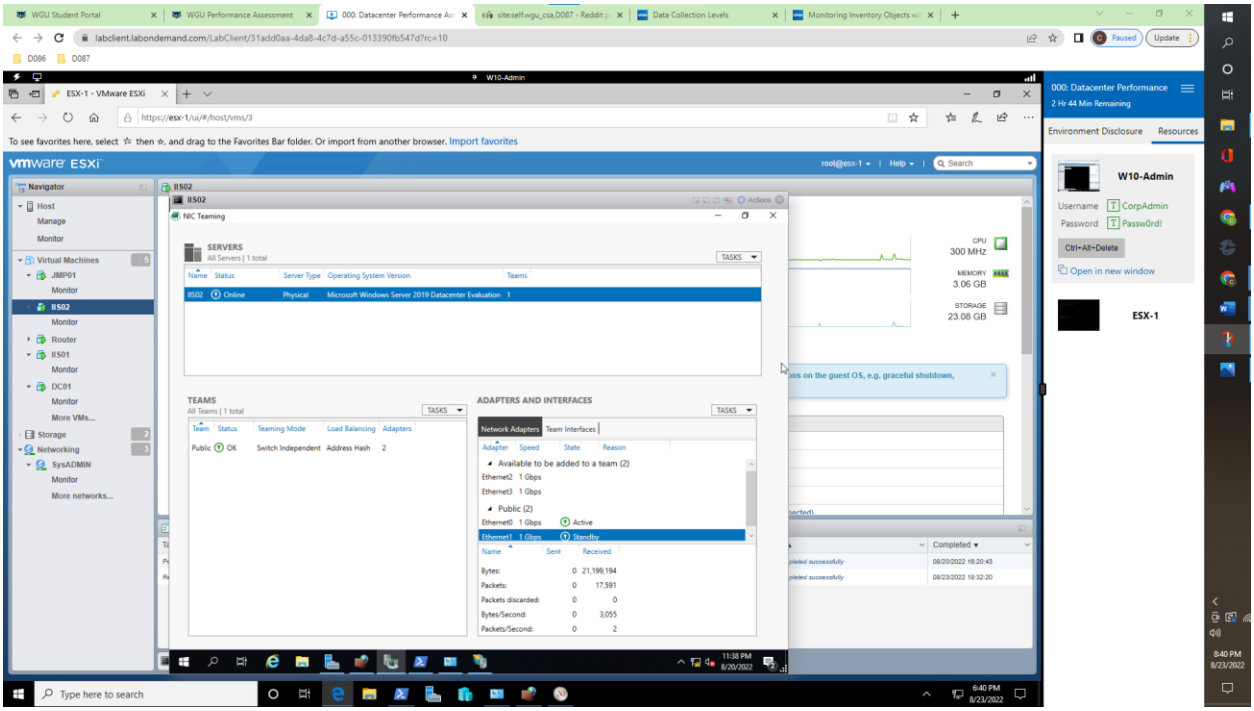
DOMAIN: Domain '*augustacrissy.lab*' configured on DC01



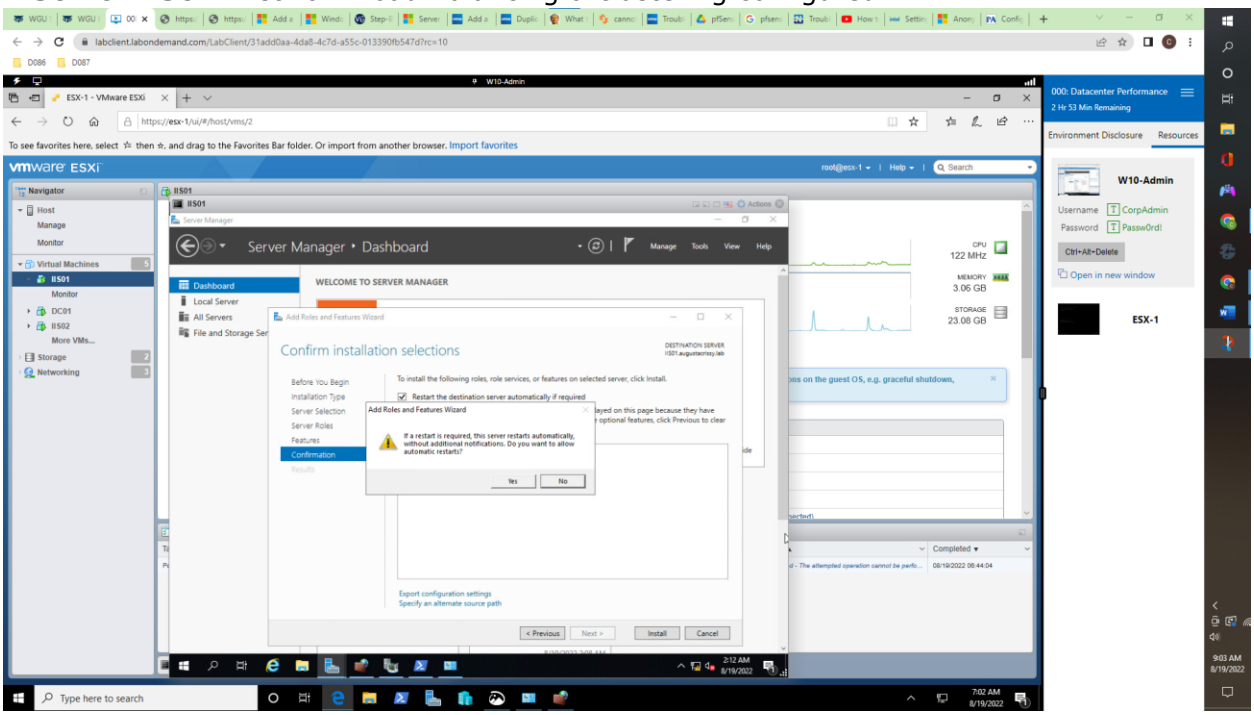
IIS01: NIC Teaming

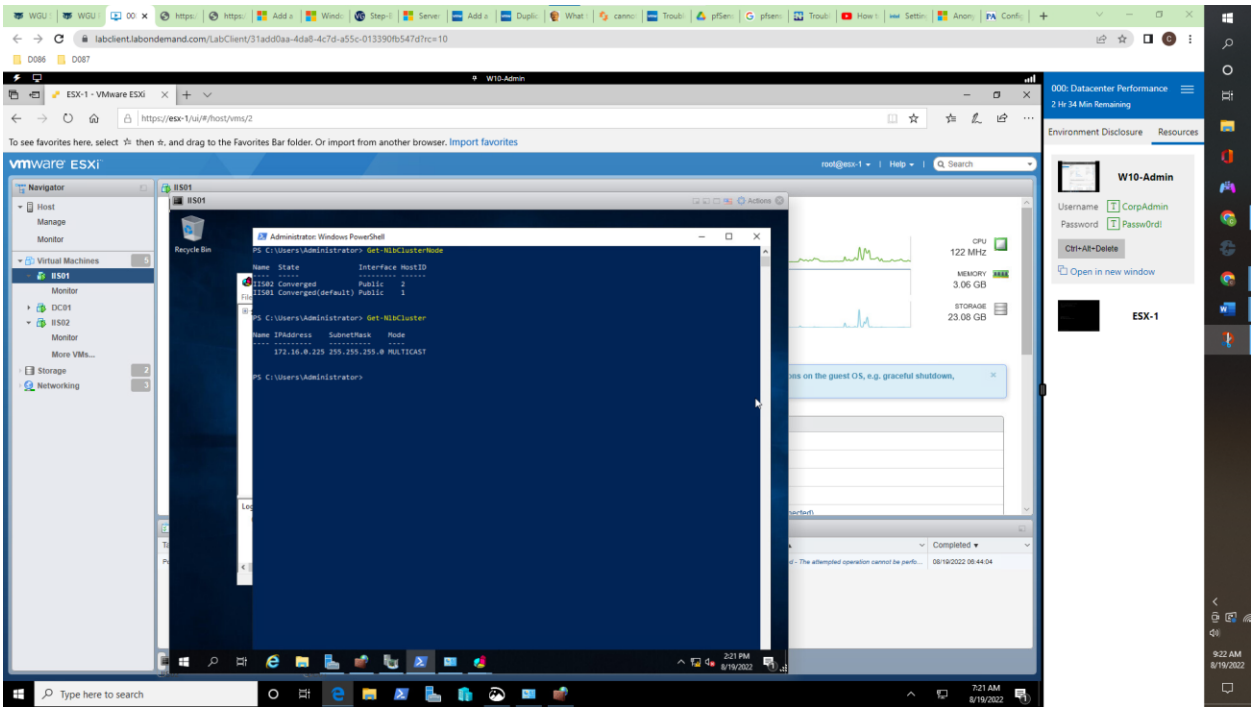


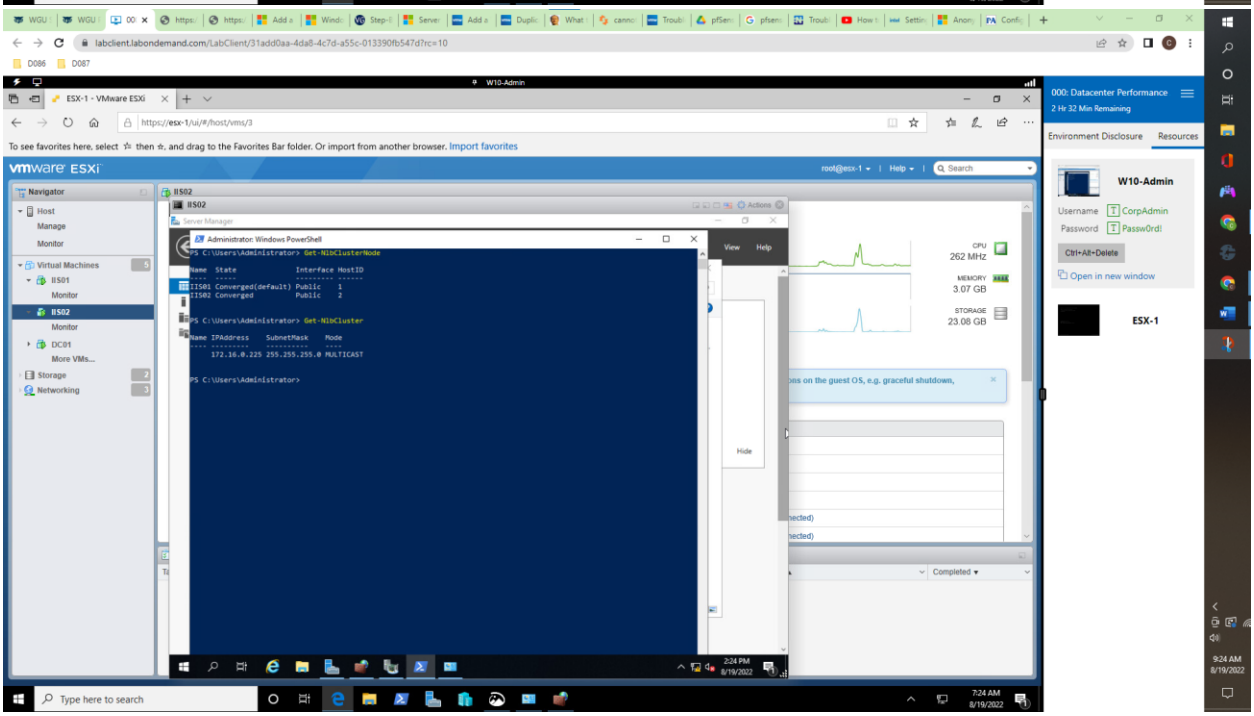
IIS02: NIC Teaming



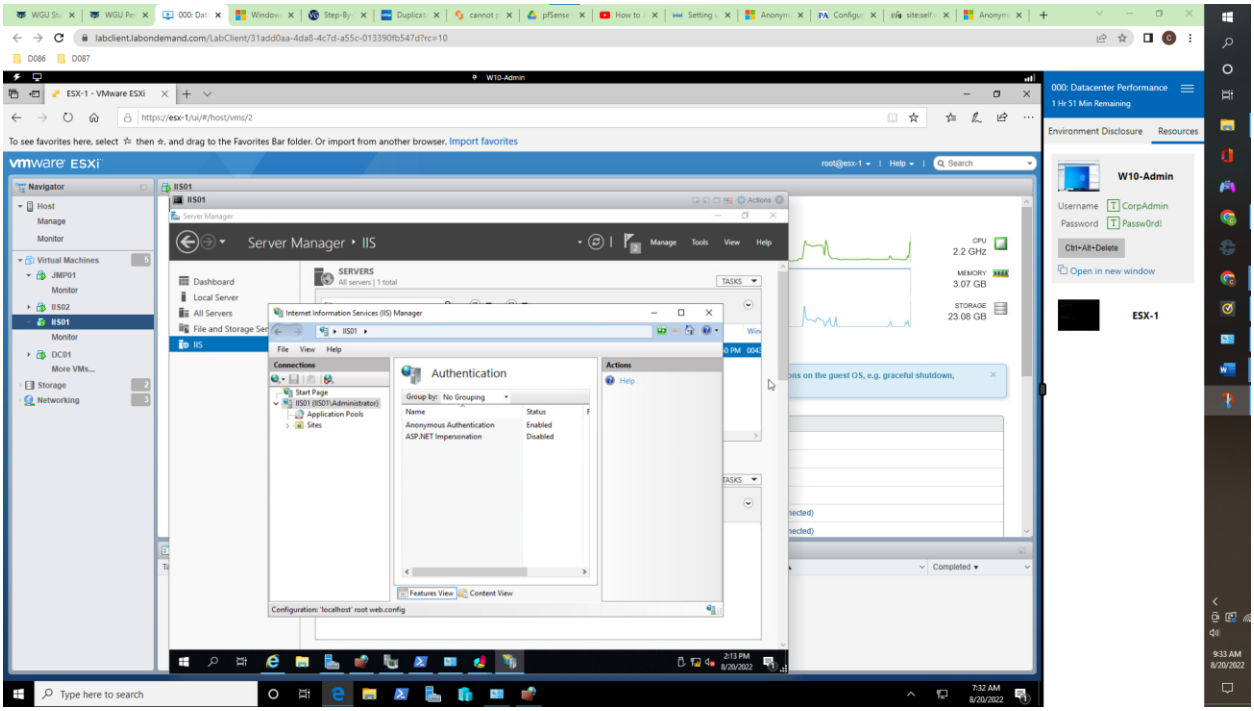
IIS01 & IIS02: Network Load Balancing & clustering configured

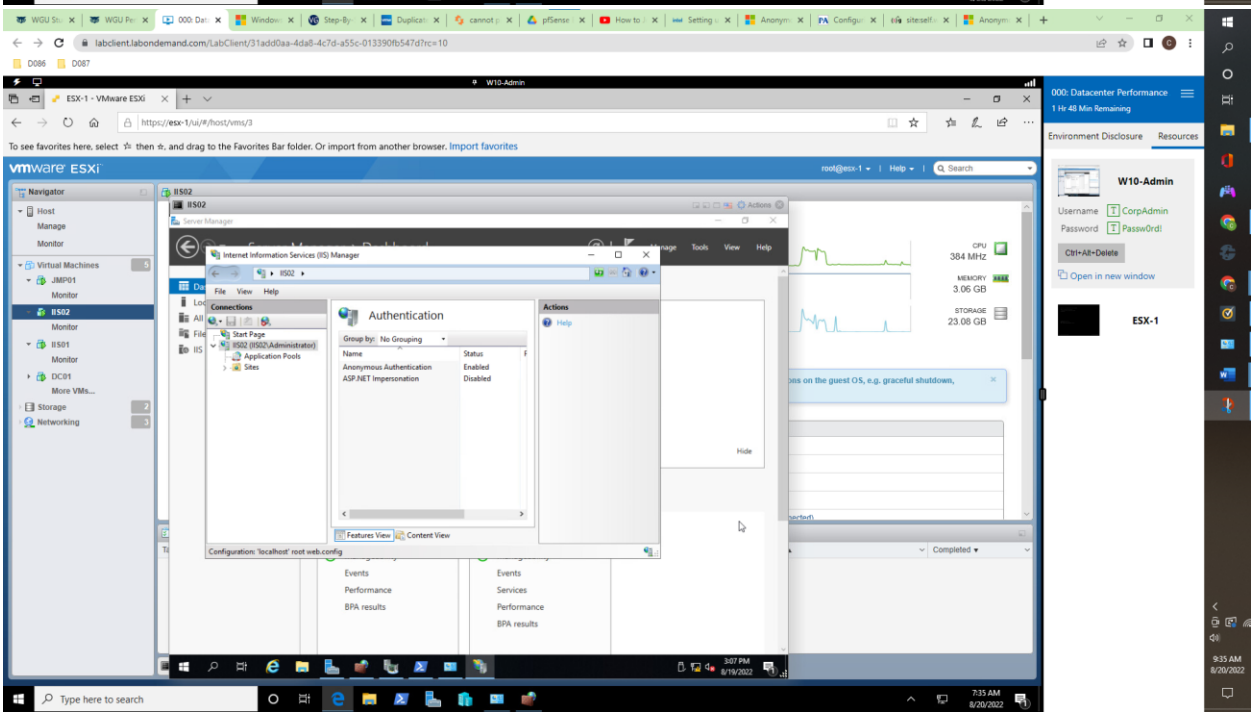



labclient.labondemand.com/LabClient/31add0aa-4da8-4c7d-a55c-013390fb547d?rc=10
ESX-1 - VMware ESXi
https://esx-1/ui/#/host/vms/2
vmware ESXi
Navigator
Host
Manage
Monitor
Virtual Machines
IIS01
IIS02
DC01
More VMs...
Storage
Networking
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-NlbClusterNode
Name State Interface HostID
IIS01 Converged Public 2
IIS02 Converged(default) Public 1
PS C:\Users\Administrator> Get-NlbCluster
Name IPAddress SubnetMask Mode
172.16.0.225 255.255.255.0 MULTICAST
PS C:\Users\Administrator>
000: Datacenter Performance
2 Hr 34 Min Remaining
Environment Disclosure
Resources
W10-Admin
Username CorpAdmin
Password Passw0rd!
Ctrl+Alt+Delete
Open in new window
ESX-1
CPU 122 MHz
MEMORY 3.06 GB
STORAGE 23.08 GB
Type here to search

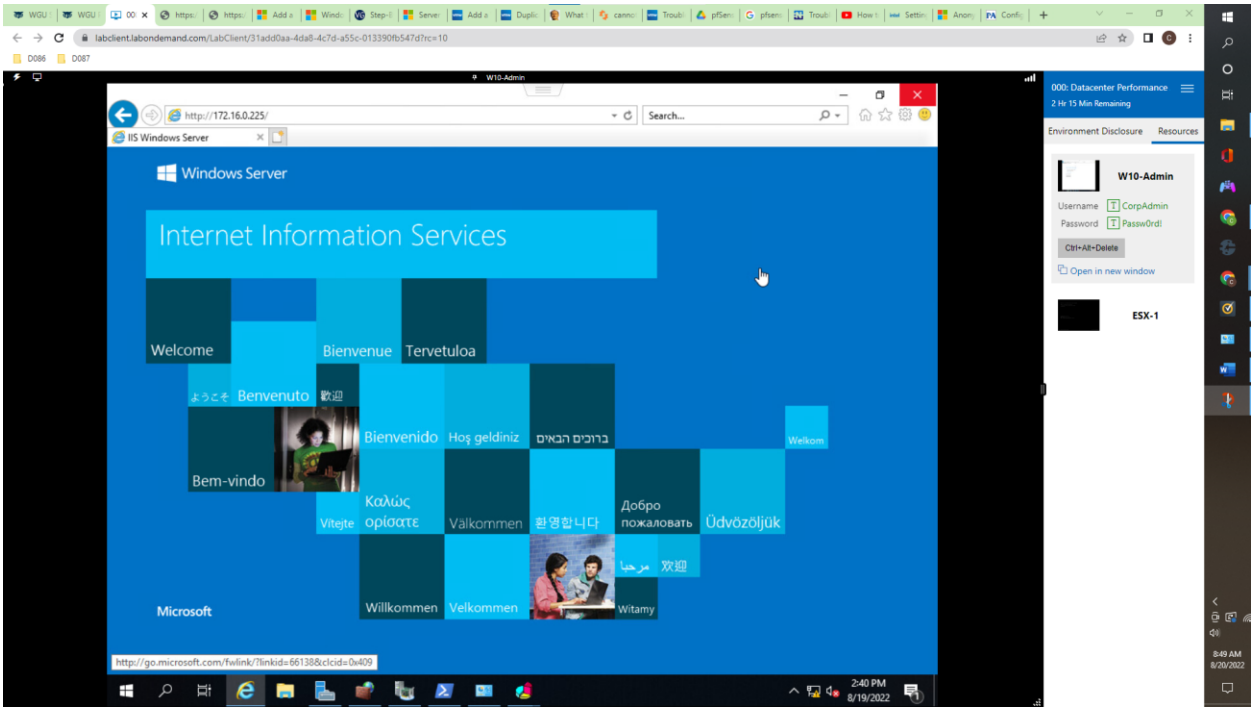

labclient.labondemand.com/LabClient/31add0aa-4da8-4c7d-a55c-013390fb547d?rc=10
ESX-1 - VMware ESXi
https://esx-1/ui/#/host/vms/3
vmware ESXi
Navigator
Host
Manage
Monitor
Virtual Machines
IIS01
IIS02
DC01
More VMs...
Storage
Networking
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-NlbClusterNode
Name State Interface HostID
IIS01 Converged(default) Public 1
IIS02 Converged Public 2
PS C:\Users\Administrator> Get-NlbCluster
Name IPAddress SubnetMask Mode
172.16.0.225 255.255.255.0 MULTICAST
PS C:\Users\Administrator>
000: Datacenter Performance
2 Hr 32 Min Remaining
Environment Disclosure
Resources
W10-Admin
Username CorpAdmin
Password Passw0rd!
Ctrl+Alt+Delete
Open in new window
ESX-1
CPU 262 MHz
MEMORY 3.07 GB
STORAGE 23.08 GB
Type here to search

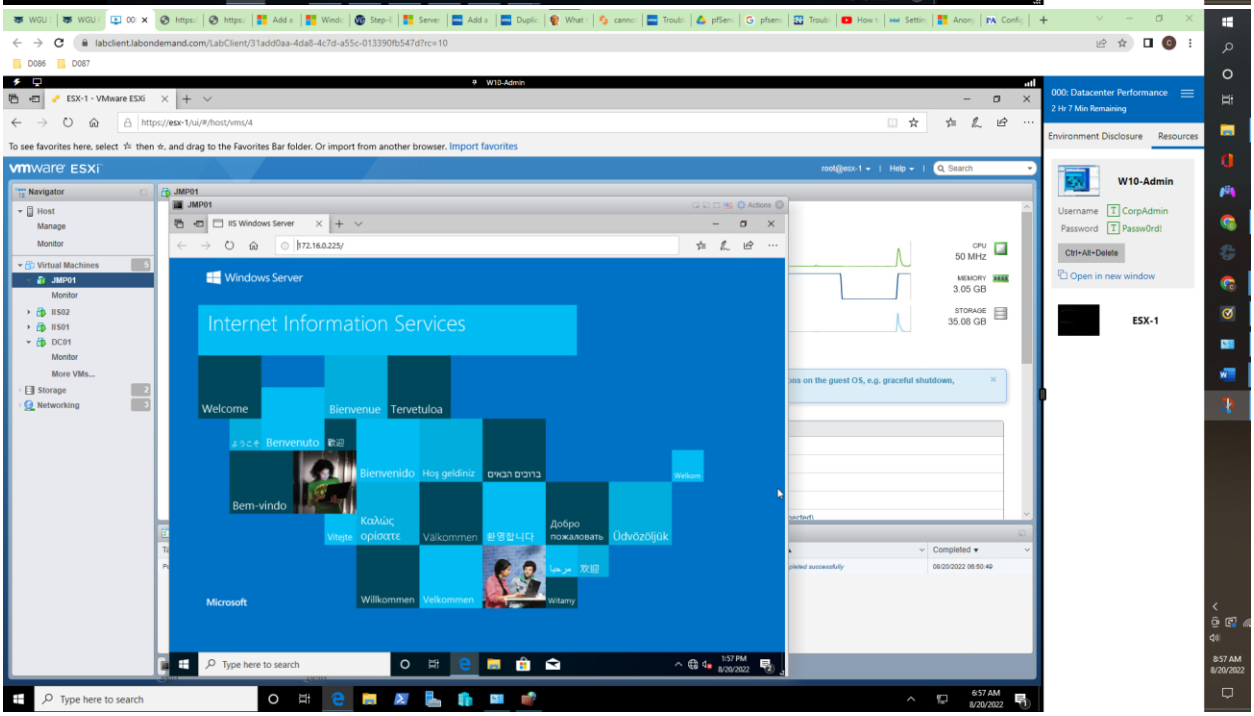
IIS01 & IIS02: Anonymous authentication enabled





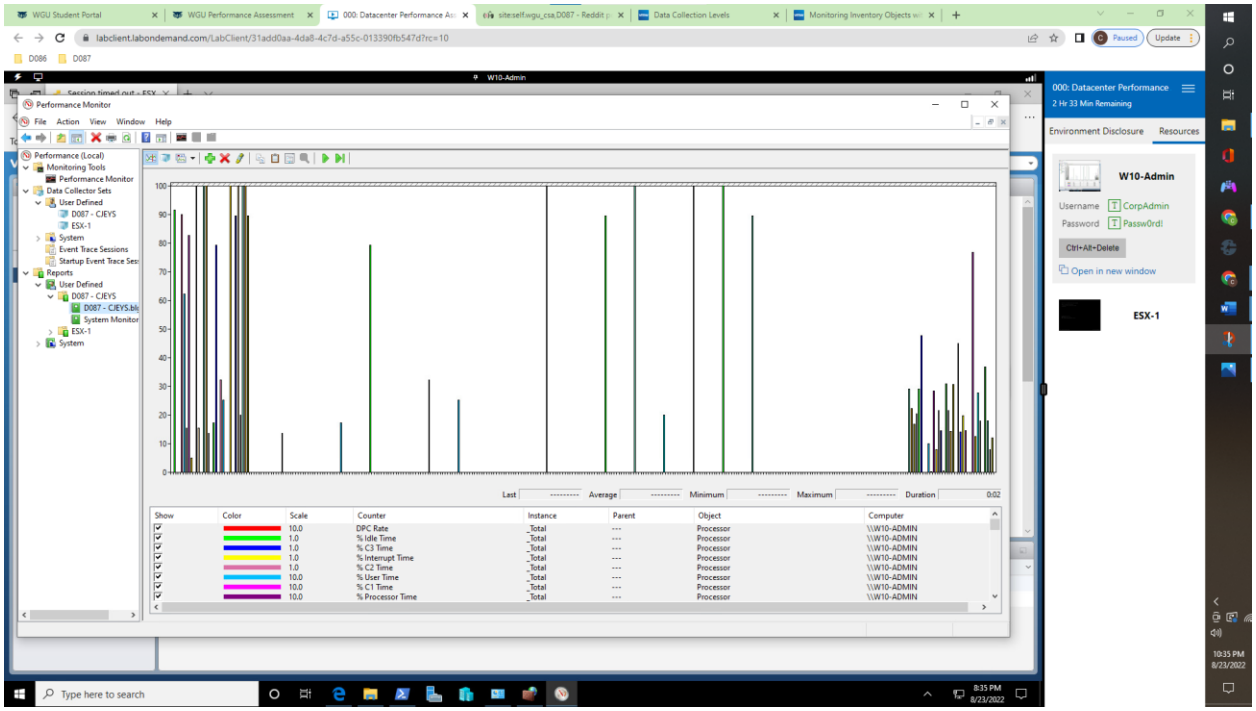
IIS: Configuration complete & accessible via JMP01





G.4. PHASE – TEST & VALIDATE

Performance Monitor: CPU utilization, network bandwidth, and memory consumption captured for reporting purposes



H. WEB SOURCES

- VMware vSphere Networking, vSwitches, Port Groups, and More!
  - https://vmiss.net/vmware-vsphere-networking/
- ISO/IEC 27001 Information Security Management
  - https://www.iso.org/isoiec-27001-information-security.html
- ISO/IEC 27001:2013 Information Security Management Standards
  - https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001
- What is information security (InfoSec)?
  - https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec
- KB00015 - Step-By-Step : How to install and configure Domain Controller on Windows Server 2019
  - https://www.virtualgyanis.com/post/step-by-step-how-to-install-and-configure-domain-controller-on-windows-server-2019
- Setting up NIC Teaming for Windows Server 2012*/2012 R2*/2016*/2019*
  - https://www.intel.com/content/www/us/en/support/articles/000022706/ethernet-products.html
- Configuring Network Load Balancing in Windows Server

- https://www.poweradmin.com/blog/configuring-network-load-balancing-in-windows-server/