

결 재	담당	원장

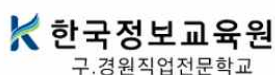
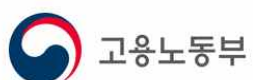
클라우드데브옵스(DevOps) 엔지니어및관리자 양성과정(8기)

2차 프로젝트 완료 보고서

- KVM 가상 서버 구축 및 관리 -

2023.07.12.(총 23일)

김학남, 박무진, 김지영



프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

목차

1. 프로젝트 개요명

(1) 프로젝트명	4
(2) 프로젝트 기간	4
(3) 프로젝트 배경 및 요구 사항	4
(4) 프로젝트 범위 및 수행 요건	5

2. 프로젝트 추진 체계

(1) 프로젝트 참여인력 총괄표	7
(2) 참여인력 업무분장	7

3. 세부 프로젝트 내용

(1) 물리적 구성	8
(2) 논리적 구성	9
(3) 상세 설계 내용	11
(4) 네트워크/소프트웨어 상세 설정	13
(5) 구축 결과	41

4. 프로젝트 일정

5. 시행 착오

6. 유지보수 계획

(1) 유지보수 개요	44
(2) 유지보수 지원	44

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

I. 프로젝트 개요

1. 프로젝트 명

KVM 가상 서버 구축 및 관리

2. 프로젝트 기간

2023.06.22. ~ 2023.07.14. (총 23일)

3. 프로젝트 배경 및 요구 사항

고객사는 현재 웹 서버 구축이 필요합니다..

- (1) 새로운 온라인 쇼핑몰을 개설하려고 합니다. 이를 위해 웹 서버를 구축하여 제품 판매와 마케팅을 위한 중요한 도구로 활용하려고 합니다.
- (2) 제한된 물리적 서버 리소스로 웹 서버를 구축해야 합니다. 이를 위해 KVM 가상화 기술을 사용하여 물리적 서버로 여러 개의 가상 서버를 호스팅할 필요가 있습니다.
- (3) 생성한 가상 서버를 효과적으로 관리하기 위한 관리 플랫폼이 필요합니다. 이를 통해 가상 서버의 집중 관리와 모니터링, 리소스 할당과 마이그레이션 등이 보다 효율적으로 수행하는 것을 기대합니다.

[요구 사항]

- ✓ KVM 구성으로 격리된 환경의 VM에서 효율적 자원 분배
- ✓ 격리된 환경의 VM으로 3-tier-web-architecture 구축으로 부하 방지 및 보안 강화
- ✓ Proxy 설정을 통해 가용성 및 부하 분산, 실제 웹 서버의 IP를 알 수 없으므로 보안 강화
- ✓ 구축한 웹 서버와 외부 인터넷 연결을 위한 네트워크 장비 구성
- ✓ PXE 구축으로 VM 자동화 설치
- ✓ OVS, VyOS를 통해 물리 서버의 VM에서 외부로의 통신
- ✓ vSphere 구축으로 인한 VM 중앙 집중적 관리 및 모니터링
- ✓ 물리 장비의 원격 접속을 위한 SSH 설정 (관리자)
- ✓ 내부 서버 대상의 취약점 공격에 대비한 보안 설정

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

4.1 프로젝트 범위

◆ Network 구성

- 이중화 구성으로 장애가 발생하더라도 서비스의 연속성 유지
- NAT 설정으로 내외부 통신 관리 및 port-forwarding으로 외부로부터 웹 서버 접속
- 물리 서버에 OpenVswitch 및 VyOS로 인해 서버 간 통신 및 격리된 환경의 VM 생성
- OSPF Routing protocol로 라우팅 정보 교환 및 최적의 경로를 결정
- LACP, Portfast, Bpdufilter, RSTP 설정으로 스위치 최적화 사용 가능 및 가용성 증진
- VxLAN 및 IPsec 설정으로 가상 터널을 이용한 암호화 통신

◆ Server 구성

- 목적에 맞는 RAID 디스크 할당 및 Rocky Linux 8.8 운영체제 설치
- KVM으로 격리된 환경을 구축하여 3Tier-Web-Architecture를 구성 및 연동
- NFS 설정으로 가상 서버 간에 공유하고 접근할 수 있는 공유 폴더를 생성
- PXE 서버를 구축하여 VM 생성 시 자동화된 운영체제 설치 및 환경설정
- Proxy 설정으로 여러 가상 웹 서버에 부하 분산하여 안정화된 웹 서버 운영 가능
- DDNS 서비스를 실행하여 IP 변경에 관계없이 도메인으로 웹 서비스 접근 가능
- DDNS script 자동 실행 등을 위해 Crontab을 설정하여 해당 작업을 주기적으로 자동 실행
- Health check 기능을 추가하여 각 가상 서버의 상태를 주기적으로 모니터링

◆ 가상머신 관리 플랫폼

- KVM 환경에서 vSphere 구축
- vCenter를 통해 가상 서버 관리 및 성능 모니터링 (중앙 집중식 관리 플랫폼)
- 보안 및 접근 제어, 스토리지 관리
- 다른 서버의 장애를 대비하여 Live Migration 설정

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

4.2 프로젝트 수행 요건

가. 개발 적용 지침 및 가이드라인

- 행정기관 클라우드 업무환경 도입 가이드(행정자치부, 2016.11)
- 민간 부문의 클라우드 도입 실무 가이드라인(방송통신위원회, 2012.12)
- 클라우드컴퓨팅 주요법령 해설서(과학기술정보통신부, 2017.11)
- 클라우드 정보보호 안내서(한국인터넷진흥원, 2017.12)
- 중소기업 보안위협 예방 및 대응가이드(한국인터넷진흥원, 2019.7)
- 중소기업 정보보호 업무가이드(한국인터넷진흥원, 2019.7)

나. 설계 및 개발 요건

- 본 프로젝트는 기 운영 중인 한국정보교육원의 인프라 환경과 연관성을 가지고 개발·구축 되어야 하며, 시범운영을 마친 후 서비스를 개시하여야 한다.
- 시스템은 추가 및 확장이 용이하도록 설계되어야 한다.
- 안정적인 서비스 운영이 가능하도록 서버는 상시적으로 동작이 가능 하도록 별도의 공간에서 운영되어야 하며 항온·항습 등을 유지할 수 있어야 한다.
- 훈련생들의 프로젝트를 위한 Instance의 생성·삭제·유지 보수 등이 용이 하도록 GUI가 제공되어야 하며 해당 UI에는 한국정보교육원을 상징할 수 있도록 설계·개발 되어야 한다.
- 훈련생 실습용 인스턴스는 인터넷 접속이 불가능 하므로 내부에서 도메인을 이용한 대시보드 접속이 가능하도록 한국정보교육원 내의 모든 PC는 2차 DNS는 10.0.0.0/8 로 설정 하여야 한다.
- 시스템의 물리적/논리적 Scale out/up에 대비하여 설계되어야 한다.

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

II. 프로젝트 추진 체계

1. 프로젝트 참여인력 총괄표

성명	소속	역할	담당업무
김학남	한국정보교육원	Project Leader	PM, 서버/네트워크 인프라 설계, 테스트
박무진	한국정보교육원	Project Assistant	서버/네트워크 인프라 구축
김지영	한국정보교육원	Project Assistant	서버 구축, 가상 서버 모니터링 설정

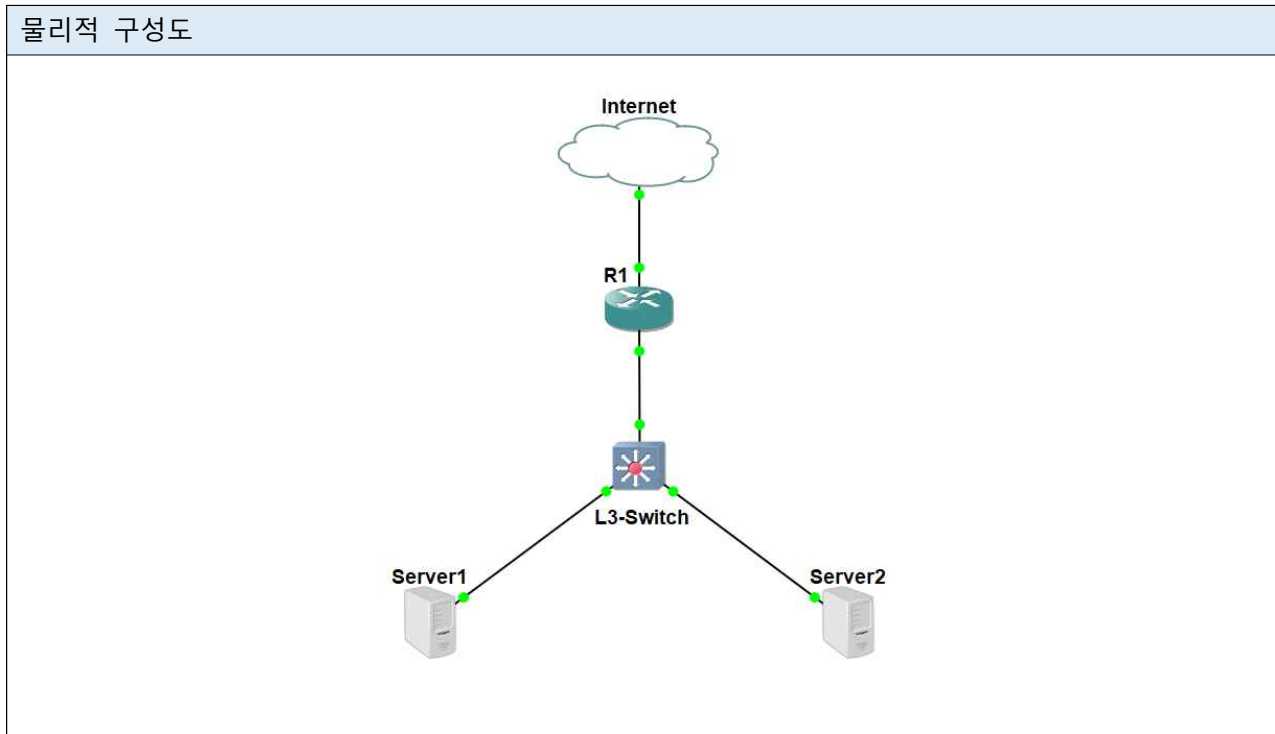
2. 참여인력 업무분장

업무명	업무내용
PM	<ul style="list-style-type: none"> - 프로젝트 수행 관리 및 책임 - 프로젝트 범위, 인원, 일정, 결과 보고 - 프로젝트 진행 상황에 따른 계획 조정 - 기타 서류, 보고서 작성 및 발표
서버/네트워크 인프라 설계/구축	<ul style="list-style-type: none"> - 서버 및 네트워크 Topology 구성 - 물리적 서버/네트워크 장비 수 산정 및 IP 설계 - 서버 리소스 설정 및 관리 - Routing protocol 결정 - KVM, vSphere 설치 및 구성 - PXE 서버 구축 및 VM 자동화 설치 - 3-Tier-Web-Architecture 구축 및 이중화 지원
3-Tier-Web- Architecture 구축	<ul style="list-style-type: none"> - 서버 및 네트워크 장비/OS 설치 지원 - MariaDB 설치 및 환경 구성 - Proxy 기능을 포함하고 있는 Nginx 설치 및 환경설정 - PHP를 설치하여 동적 웹 페이지를 생성하기 위해 Nginx와 연동 - Web, PHP proxy 구성
가상 서버 모니터링 설정	<ul style="list-style-type: none"> - vCenter 설치 및 호스트 구성 - nested KVM 설정 - ESXi 내부 가상 서버 구축 - Live Migration 체크 - VM 생성용 Template 제작
테스트 및 검토	<ul style="list-style-type: none"> - 고객사의 요구사항 충족 확인 - 구축에 따른 단계별 산출물 검토

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

Ⅲ. 세부 프로젝트 내용

(1) 물리적 구성



가) 장비

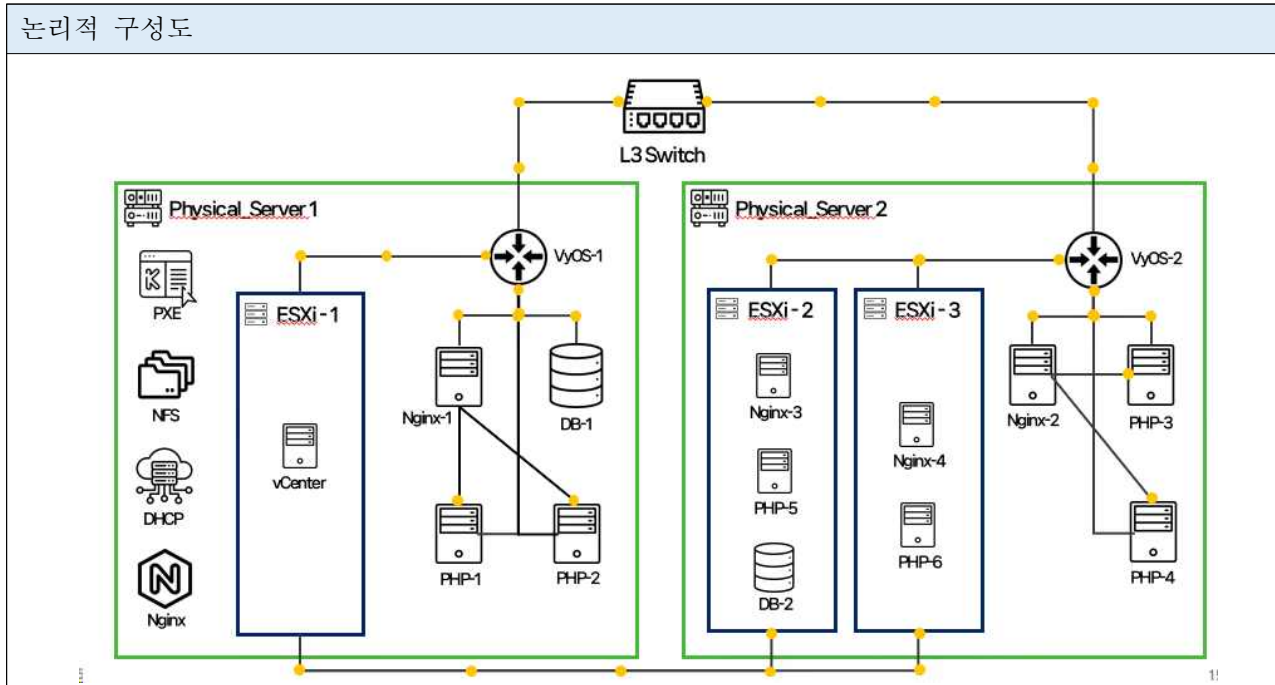
H/W	장비명	개수	비고
Physical Router	CISCO2911/K9	1	
Physical Switch	WS-C3750X-24T-S	1	
Physical Server	HP Proliant DL360 G7	2	Rocky linux 설치 및 Raid 0, Raid 5 적용 (입출력 속도와 안정성 증가)

나) 물리적 구성

- Direct UTP cable 제작 후 다른 계층 장비 간 연결
- L3 스위치에 각각 Router와 Server 2대를 연결
- 각 Server는 3개의 Link로 L3 스위치와 연결한 후 LACP Link aggregation 설정(Loop 방지 및 가용성)
- 각 Server에 다른 VLAN access 설정한 후 L3 스위치에서 라우팅
- 관리자의 원격 접속을 위한 전용 IP 설계와 SSH 설정

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

(2) 논리적 구성



가) OS, SW

Server OS	Rocky Linux 8.8
Hypervisor OS	KVM 6.2.0, vSphere 6.7
OpenVswitch	openvswitch2.17
VyOS	v1.3.2
WEB	Nginx 1.22.1
PHP	PHP 7.4.33, PHP 8.2.9
DB	MariaDB 10.6.15
SSH terminal	MobaXterm Professional Edition 22.3, SecureCRT 8.5

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

나) 논리적 구성

- L3 스위치에서 각 서버에 접근 가능한 VLAN을 각각 VLAN10, VLAN20으로 지정 및 SVI 설정
- OSPF Routing Protocol 선언
- Router에서 NAT 설정하여 보안성 강화
- Portfast, Bpdufilter
- 물리 서버에 Rocky Linux OS 설치 및 RAID 디스크 할당
- KVM 서버 구축
 - 3Tier-Web-Architecture(Nginx-PHP-DB) 구축
 - EXSi 가상 서버 3대 구축 및 vCenter 설치하여 생성된 호스트를 중앙 집중식 관리
- 각 서버의 ovs-VLAN30 네트워크는 VxLAN L2 tunneling을 통해 서로 통신. 여기에 IPsec 암호화 통신 설정
- VyOS를 설정하여 물리 서버 내부의 가상 서버 또한 Routing protocol로 외부 통신
- PXE 서버 구축
 - NFS : Server1의 /web 공유디렉토리로 사용
 - DHCP : VM 생성 시 해당 VM의 IP 자동 할당
 - Kickstart : VM 생성 시 효율적인 자동화 OS 설치 및 환경설정
- Web Proxy : Server1과 Server2에 각각 존재하는 Nginx 가상 서버로 부하 분산
- PHP Proxy : 각 Nginx 가상 서버 1대당 PHP 가상 서버 2대가 연동되어 부하 분산 (timeout 3초 설정)
- DDNS & Crontab : www.haknam.shop 도메인의 IP주소가 변경되더라도 해당 도메인만으로 변경된 IP를 찾아갈 수 있게 설정함. Crontab으로 DDNS shell script를 5분마다 주기적으로 실행함
- Health Check : Server1의 nginx-1 가상 서버에서 health check shell script를 생성 및 실행하여 주기적으로 PHP 가상 서버들의 상태 체크

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

(3) 상세 설계 내용

물리 서버 디스크 설정		
Server1 (RAID 0)	약 500GB (디스크 2개)	/boot : 1GB
		swap : 10GB
		/root : 나머지
Server2 (RAID 5)	약 750GB (디스크 3개)	/boot : 1GB
		swap : 10GB
		/root : 나머지

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12


서버 및 네트워크 장비의 IP 설정			
Router	int g0/0	인터넷 연결 포트	DHCP
	int g0/1	스위치 연결 포트	ip 192.168.100.1/24
	int g0/2	스위치 Management VLAN99 연결 포트	ip 10.10.11.1/8
Switch	int g1/0/1	Router 연결 포트	ip 192.168.100.2/24
	int vlan 99	Management 네트워크 연결 포트	ip 10.10.11.2/8
	int vlan 10	Server1 연결 포트	ip 192.168.101.251/24
	int vlan 20	Server2 연결 포트	ip 192.168.102.252/24
Server 1	enp4s0f1	스위치 Management VLAN999 연결 포트	ip 10.10.11.10/8 gw 10.0.0.1
	ovs0	스위치 VLAN10 연결 포트	ip 192.168.101.10/24
	ovs0-vlan30	VLAN30 서버 연결	ip 172.16.101.10/24
	ovs0-vlan40	VLAN40 서버 연결	ip 172.16.102.10/24
Server 2	enp4s0f1	스위치 Management VLAN999 연결 포트	ip 10.10.11.20/8 gw 10.0.0.1
	ovs0	스위치 VLAN20 연결 포트	ip 192.168.101.20/24
	ovs0-vlan30	VLAN30 서버 연결	ip 172.16.101.20/24
	ovs0-vlan50	VLAN50 서버 연결	ip 172.16.103.30/24
VyOS1	eth0	ovs0 네트워크의 게이트웨이	ip 192.168.101.11/24
	eth1	VLAN30 네트워크의 게이트웨이	ip 172.16.101.254/24
	eth2	VLAN50 네트워크의 게이트웨이	ip 172.16.102.254/24
VyOS2	eth0	ovs0 네트워크의 게이트웨이	ip 192.168.102.21/24
	eth1	VLAN30 네트워크의 게이트웨이	ip 172.16.101.253/24
	eth2	VLAN50 네트워크의 게이트웨이	ip 172.16.103.253/24

※ 상세 IP 정리는 PPT 참고 (가상머신 IP 포함)

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

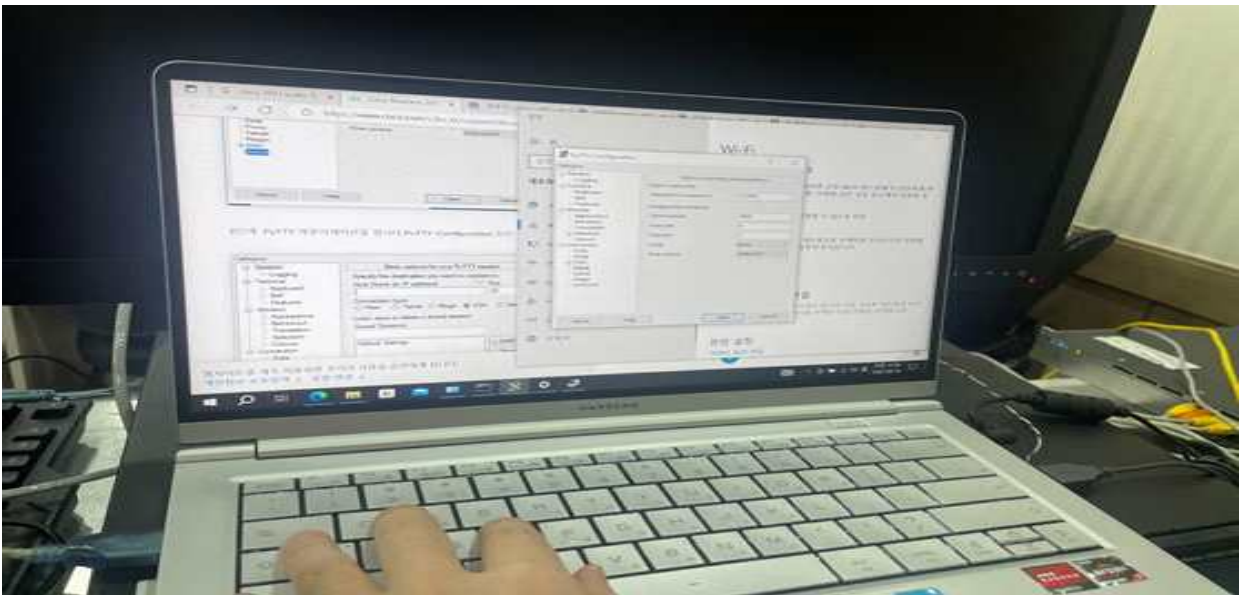
(4) 네트워크/소프트웨어 상세 설정

케이블 제작 및 장비 연결 (Router, L3 Switch, Server1, Server2)



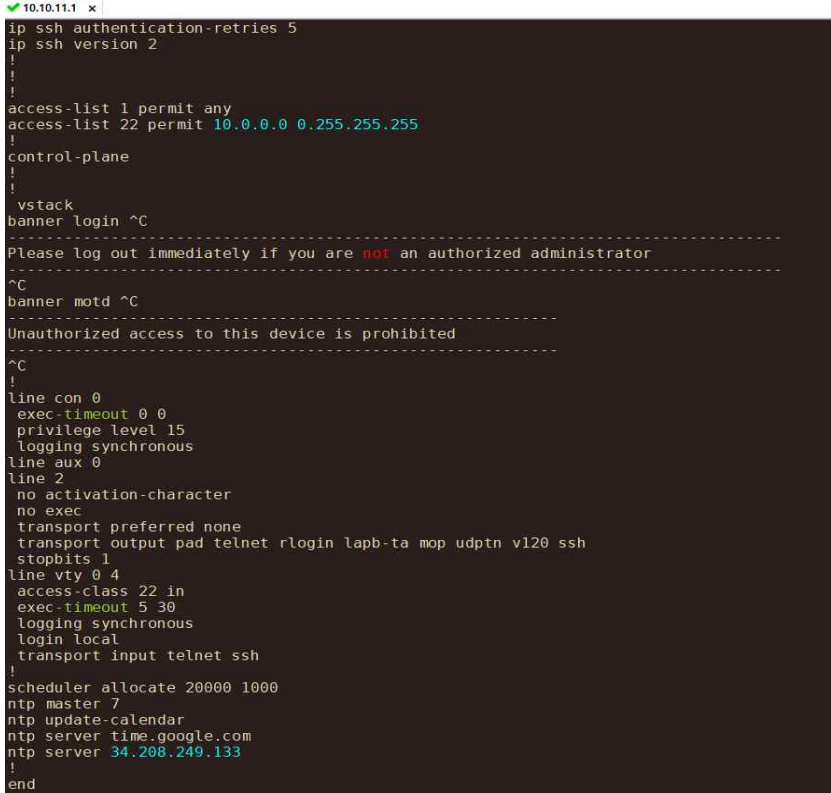
- Router 1대, L3 Switch 1대, Physical Server 2대
- Direct UTP cable 제작
- 서로 다른 계층 장비끼리 연결

네트워크 장비 Console 접속 (Router, L3 Switch)



- Putty(터미널)을 이용하여 Router와 L3 Switch에 console 접속 및 IP 설정

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

SSH 및 ACL (Router)
 <pre> 10.10.11.1 x ip ssh authentication-retries 5 ip ssh version 2 ! ! access-list 1 permit any access-list 22 permit 10.0.0.0 0.255.255.255 ! control-plane ! ! vstack banner login ^C ----- Please log out immediately if you are not an authorized administrator ----- ^C banner motd ^C ----- Unauthorized access to this device is prohibited ----- ^C ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 line 2 no activation-character no exec transport preferred none transport output pad telnet rlogin lapb-ta mop udptn v120 ssh stopbits 1 line vty 0 4 access-class 22 in exec-timeout 5 30 logging synchronous login local transport input telnet ssh ! scheduler allocate 20000 1000 ntp master 7 ntp update-calendar ntp server time.google.com ntp server 34.208.249.133 ! end </pre>
<ul style="list-style-type: none"> - Router에 ACL & SSH설정 - 관리용 IP(10.10.11.0/8)으로만 SSH 접속 가능하도록 ACL 설정 - 접속 재시도 횟수 5회로 제한 - 내부 장비를 관리하기 위해 각 장비에 원격으로 접속할 필요가 있어 원격 암호화 접속 SSH 사용 - ACL : 컴퓨터 시스템 및 네트워크 장비에서 접근 제어를 관리하기 위해 사용 - SSH 접속 IP 대역 <ul style="list-style-type: none"> - Router 10.10.11.1 - L3 Switch 10.10.11.2 - Server1 10.10.11.10 - Server2 10.10.11.20 - 설정한 관리용 IP 대역으로만 장비에 원격 접속을 허용 - 다른 내부 IP로는 원격 접속 불가능

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

NAT (Router)
<pre> R1#sh run sec nat ip nat outside ip nat inside default-information originate ip nat inside source list 1 interface GigabitEthernet0/0 overload ip nat inside source static tcp 192.168.101.10 80 interface GigabitEthernet0/0 80 access-list 1 permit any </pre>
<ul style="list-style-type: none"> - Router에 ACL로 내부의 모든 IP대역 지정 - Web Proxy 가상 서버가 있는 Server 1 IP로 Port forwarding 설정하여 외부에서 접속 가능 <ul style="list-style-type: none"> - 외부망에서 내부 사설 네트워크에 상주하는 Web 서버 호스트에 대한 서비스 생성 가능 - NAT : 내부에서 외부로의 통신은 자유롭게 되지만 외부에서 내부로의 통신은 차단하여 네트워크 보안성 향상 IP 주소 부족 대응, 익명성 제공, 트래픽 관리

OSPF (Router)
<pre> S* 0.0.0.0/0 [254/0] via 175.197.24.254 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.0.0.0/8 is directly connected, GigabitEthernet0/2 L 10.10.11.1/32 is directly connected, GigabitEthernet0/2 125.0.0.0/32 is subnetted, 1 subnets S 125.141.115.26 [254/0] via 175.197.24.254, GigabitEthernet0/0 172.16.0.0/24 is subnetted, 3 subnets O IA 172.16.101.0 [110/3] via 192.168.100.2, 17:06:59, GigabitEthernet0/1 O IA 172.16.102.0 [110/3] via 192.168.100.2, 17:06:59, GigabitEthernet0/1 O IA 172.16.103.0 [110/3] via 192.168.100.2, 19:48:11, GigabitEthernet0/1 175.197.0.0/16 is variably subnetted, 2 subnets, 2 masks C 175.197.24.0/24 is directly connected, GigabitEthernet0/0 L 175.197.24.178/32 is directly connected, GigabitEthernet0/0 192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.100.0/24 is directly connected, GigabitEthernet0/1 L 192.168.100.1/32 is directly connected, GigabitEthernet0/1 O 192.168.101.0/24 [110/2] via 192.168.100.2, 17:06:59, GigabitEthernet0/1 O 192.168.102.0/24 [110/2] via 192.168.100.2, 19:48:11, GigabitEthernet0/1 interface GigabitEthernet0/1 ip address 192.168.100.1 255.255.255.0 ip nat inside ip virtual-reassembly in ip ospf 1 area 0 duplex full speed auto </pre>
<ul style="list-style-type: none"> - Router에 L3 Switch와 연결되어 있는 인터페이스를 OSPF area 0로 선언 - Router에 Server1과 Server 2의 IP네트워크 대역을 OSPF로 통신 - 외부 인터넷과 연결된 포트를 default-gateway로 설정 <ul style="list-style-type: none"> - default-information originate : default-routing 재분배 설정, 다른 서버에서도 외부 인터넷과 통신 - OSPF : 최적화, 스케일링, 동적 경로 선택, 고가용성 및 회복성, 변경관리, 대규모 네트워크 관리

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

LACP (Link aggregation) (L3 Switch)					
<pre> Number of channel-groups in use: 2 Number of aggregators: 2 Group Port-channel Protocol Ports -----+-----+-----+----- 1 Po1(SU) LACP Gi1/0/5(P) Gi1/0/7(P) Gi1/0/9(P) 2 Po2(SU) LACP Gi1/0/6(P) Gi1/0/8(P) Gi1/0/10(P) </pre>					
<ul style="list-style-type: none"> - 각 Server와 연결되어 있는 3개의 physical port를 bonding(LACP) - PO1 : Physical Server1과 연결, PO2 : Physical Server2와 연결 - LACP : 회선의 대역폭 증가, 장애 조치 및 신뢰성 향상, 자동 설정, 루프 방지 등의 이점 					

VLAN (L3 Switch)			
VLAN	Name	Status	Ports
1	default	active	Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23
10	VLAN0010	active	Po1
20	VLAN0020	active	Po2
999	VLAN0999	active	Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/24
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinet-default	act/unsup	
1005	trnet-default	act/unsup	
<ul style="list-style-type: none"> - 각 물리 서버 2대는 서로 다른 곳에 있다고 가정하였음. Server1은 VLAN10으로 Access설정, Server2에는 VALN20으로 설정하여 각 독립적인 네트워크 환경 구성 (Broadcast Domain을 분할) - VLAN이 동일한 포트끼리만 데이터 전달을 허용 - VLAN999는 관리자 접속용 : G1/0/2(Router), G1/0/3(Server1), G1/0/4(Server2), G1/0/24 (인터넷선) - VLAN : 네트워크분리, 보안강화, 효율적인 네트워크관리, 물리적 리소스공유, 가상화지원 			

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

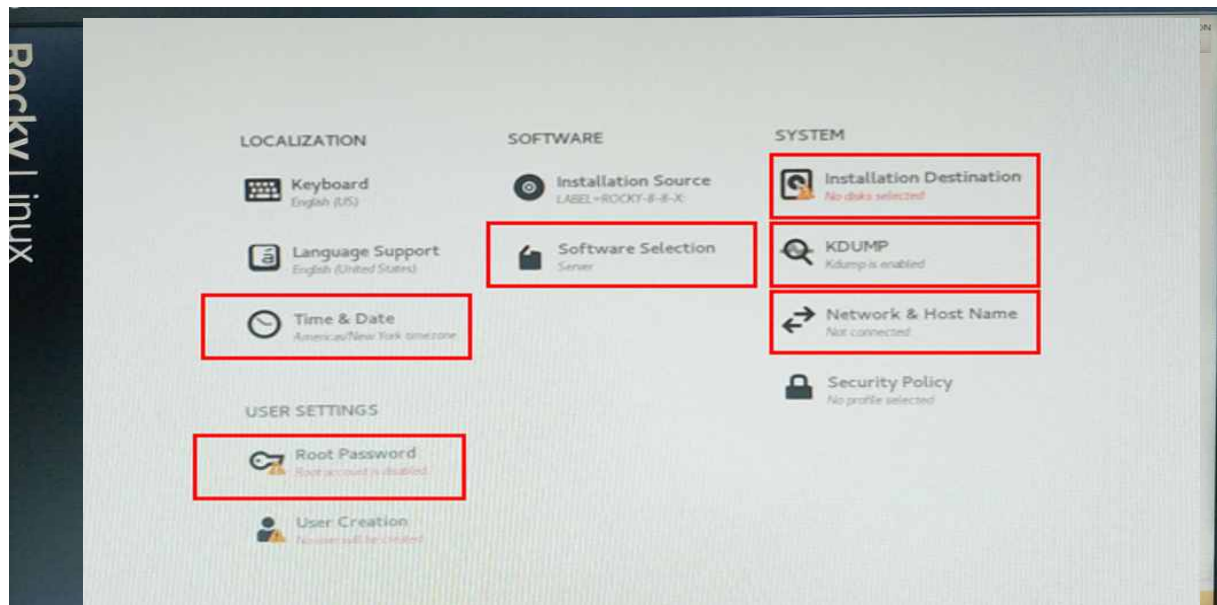
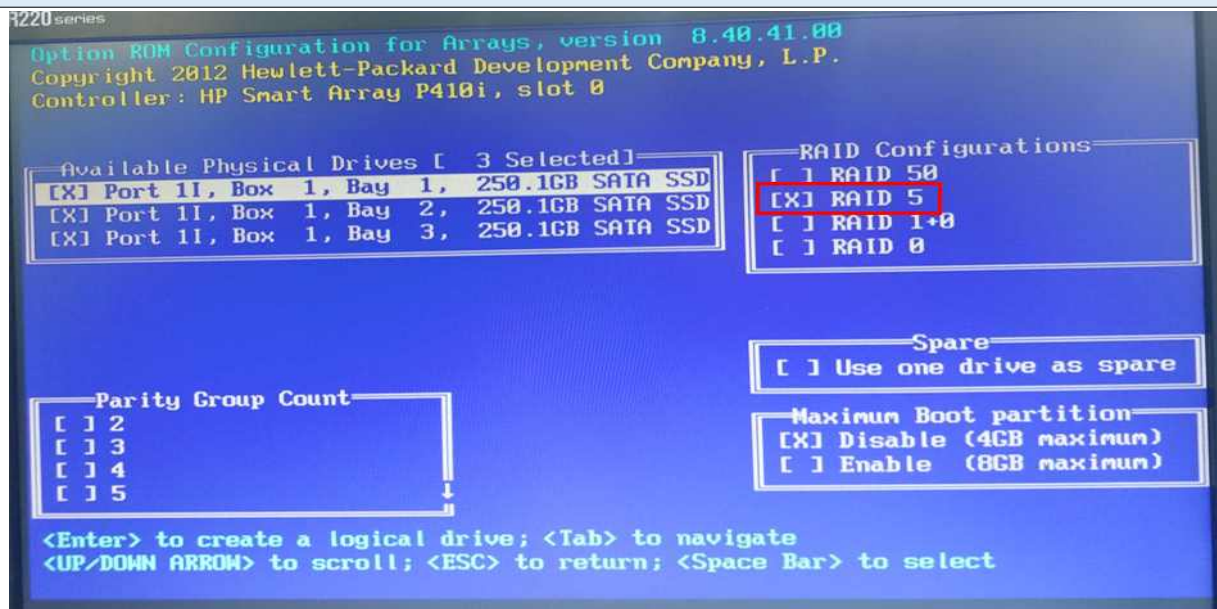
OSPF(L3 Switch)	
<pre> 0*E2 0.0.0.0/0 [110/1] via 192.168.100.1, 1d04h, GigabitEthernet1/0/1 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.0.0.0/8 is directly connected, Vlan999 L 10.10.11.2/32 is directly connected, Vlan999 172.16.0.0/24 is subnetted, 3 subnets O IA 172.16.101.0 [110/2] via 192.168.102.21, 08:12:12, Vlan20 O IA 172.16.102.0 [110/2] via 192.168.101.11, 08:12:12, Vlan10 O IA 172.16.103.0 [110/2] via 192.168.102.21, 08:12:12, Vlan20 192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.100.0/24 is directly connected, GigabitEthernet1/0/1 L 192.168.100.2/32 is directly connected, GigabitEthernet1/0/1 192.168.101.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.101.0/24 is directly connected, Vlan10 L 192.168.101.251/32 is directly connected, Vlan10 192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.102.0/24 is directly connected, Vlan20 L 192.168.102.252/32 is directly connected, Vlan20 interface Vlan10 ip address 192.168.101.251 255.255.255.0 ip ospf 1 area 0 interface Vlan20 ip address 192.168.102.252 255.255.255.0 ip ospf 1 area 0 interface Vlan999 ip address 10.10.11.2 255.0.0.0 ip ospf 1 area 10.10.11.0 L3-Switch#sh ip ospf neig </pre>	
<pre> Neighbor ID Pri State Dead Time Address Interface 192.168.100.1 1 FULL/BDR 00:00:32 192.168.100.1 GigabitEthernet1/0/1 192.168.101.11 1 FULL/BDR 00:00:37 192.168.101.11 Vlan10 192.168.101.0 1 FULL/BDR 00:00:32 192.168.102.21 Vlan20 </pre>	
<ul style="list-style-type: none"> - VLAN10 SVI와 VLAN20 SVI를 OSPF Area 0을 선언하여 Server1과 Server2의 IP를 라우터에 Routing table에 등록 - 관리용 SVI (VLAN999)은 다른 Area(10.10.11.0)로 선언 - 관리용 인터페이스 : passive-interface 설정하여 불필요한 hello packet 차단 및 다른 프로젝트 참여 팀과 OSPF neighbor를 맺지 않음 - Default route정보를 OSPF로 전달 	

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

Portfast, BPDUfilter (L3 Switch)	
<pre> interface Port-channel1 switchport access vlan 10 switchport mode access spanning-tree portfast edge spanning-tree bpdufilter enable interface Port-channel2 switchport access vlan 20 switchport mode access spanning-tree portfast edge spanning-tree bpdufilter enable interface GigabitEthernet1/0/2 switchport access vlan 999 switchport mode access duplex full spanning-tree portfast edge spanning-tree bpdufilter enable interface GigabitEthernet1/0/3 switchport access vlan 999 switchport mode access spanning-tree portfast edge spanning-tree bpdufilter enable interface GigabitEthernet1/0/4 switchport access vlan 999 switchport mode access spanning-tree portfast edge spanning-tree bpdufilter enable </pre>	
<ul style="list-style-type: none"> - Portfast : 해당 인터페이스는 Listening, Learning 상태를 거치지 않고 “no shutdown” 입력 시 “UP” 상태로 변경. - BPDUfilter : 종단 장치엔 BPDU를 송신할 필요가 없어서 BPDU를 보내지 않는다. - 관리자 접속용 물리 인터페이스와 물리 서버 2대에 연결되어 있는 링크 통합 인터페이스에 설정 	

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

RAID 구성 및 Linux 설치 (Server1, Server2)



- RAID 구성
 - server1는 RAID 0 으로 구성 (250GB 물리 디스크 2개)
 - server2는 RAID 5 으로 구성 (250GB 물리 디스크 3개)
- Rocky Linux8.8설치
 - disk 설정
 - /boot는 1GB 분배
 - swap는 10GB 분배
 - /(root)는 나머지 용량 분배

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

OpenVswitch & LACP (Server1, Server2)

```
[root@server1 ~]# nmcli con show
NAME                                UUID                                TYPE                                DEVICE
ovs0-if                            befacf99-ca4e-44b4-9063-a5821a60bf7c ovs-interface                    ovs0
enp3s0f0                           6d9dbfbc-56fd-41f2-a572-75d59f59e7ce ethernet                        enp3s0f0
vlan30                             355bc3ae-213e-45c9-9f3b-02d18a0a94cd ovs-interface                    vlan30
vlan40                             d6a5542f-9757-4d8e-8455-bfd2ca4463f8 ovs-interface                    vlan40
virbr0                             43bb92fc-9468-44e6-a09e-a6f21f2f3997 bridge                          virbr0
ovs0                                c17e55df-810a-4e06-9b3a-2e4786ee5fee ovs-bridge                      ovs0
ovs0-port                          85edaa7d-8f52-4af9-b915-dbd86386d808 ovs-port                        ovs0
ovs0-vlan30                        79c83b70-61ae-4c7f-8df8-4ed430231bc8 ovs-port                        vlan30
ovs0-vlan40                        aa9c7423-83c0-419f-803e-5522410b3df1 ovs-port                        vlan40
ovs-slave-bond0                    40a15692-bd8e-4e02-98bb-12625987f24f ovs-port                        bond0
ovs-slave-enp3s0f1                 83b452f4-cc70-4fb1-8c09-aed3a160742a ethernet                        enp3s0f1
ovs-slave-enp4s0f0                 75717a33-3a62-4a0e-be20-5dbefd683157 ethernet                        enp4s0f0
ovs-slave-enp4s0f1                 40d36491-adc0-4de8-92e5-5f06040ab80a ethernet                        enp4s0f1
```

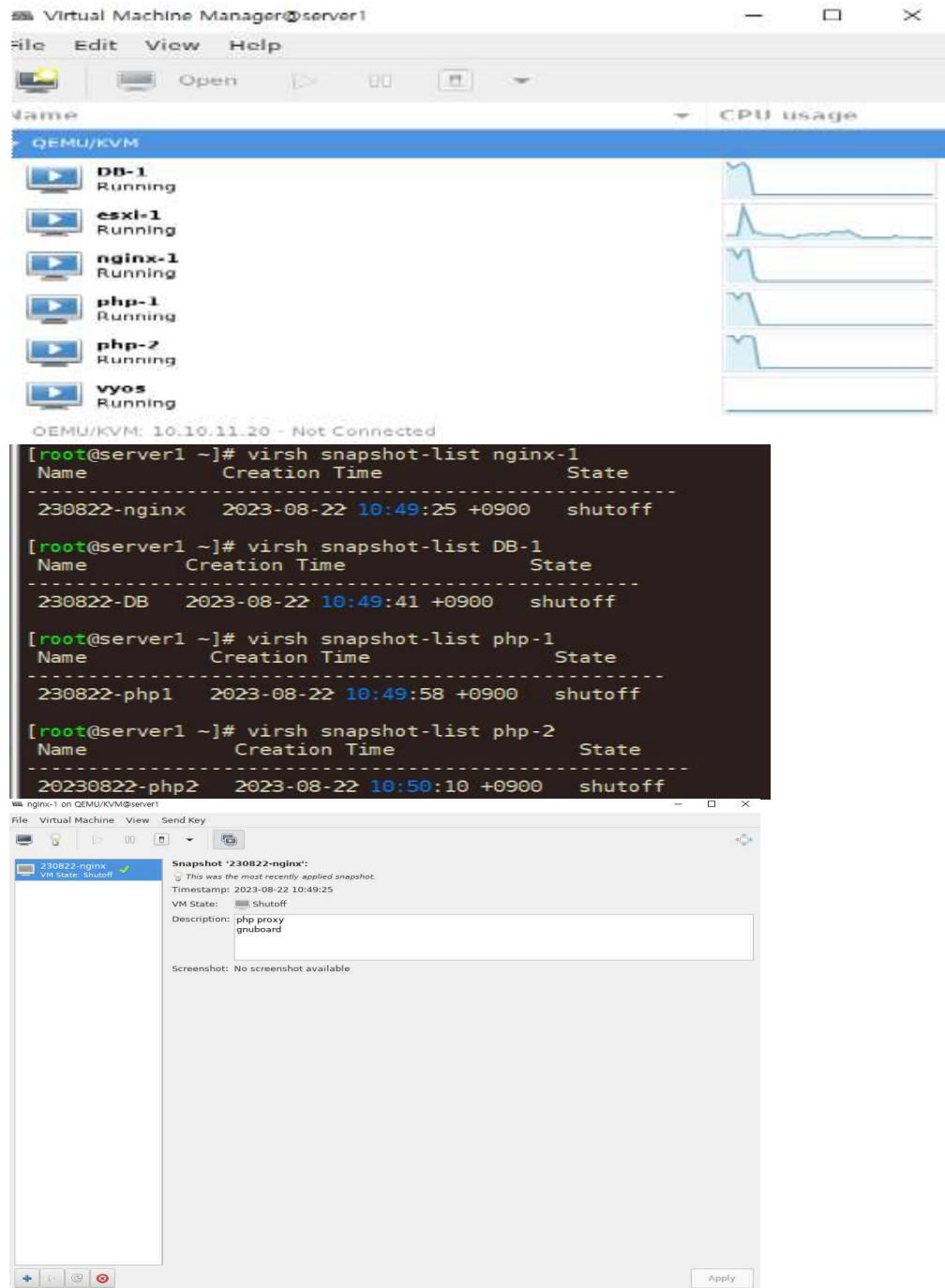
```
[root@server1 ~]# ovs-appctl bond/show bond0
---- bond0 ----
bond_mode: balance-tcp
bond_may use recirculation: yes, Recirc-ID : 1
bond-hash-basis: 0
lb_output action: disabled, bond-id: -1
updelay: 0 ms
downdelay: 0 ms
next rebalance: 353 ms
lacp_status: negotiated
lacp_fallback_ab: false
active-backup primary: <none>
active member mac: 3c:4a:92:e8:2d:36(enp4s0f1)
```

```
57: ovs0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1000
    link/ether 3c:4a:92:e8:2d:36 brd ff:ff:ff:ff:ff:ff
    inet 192.168.101.10/24 brd 192.168.101.255 scope global enp3s0f1
        valid lft forever preferred lft forever
    inet6 fe80::6dc0:f110:fc5d:ff8f/64 scope link
        valid lft forever preferred lft forever
58: vlan40: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1000
    link/ether ae:e6:39:ef:53:fb brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.10/24 brd 172.16.102.255 scope global enp4s0f1
        valid lft forever preferred lft forever
    inet6 fe80::1e56:9287:f79f:7ea8/64 scope link
        valid lft forever preferred lft forever
59: vlan30: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1000
    link/ether 46:1f:b2:31:ca:ca brd ff:ff:ff:ff:ff:ff
    inet 172.16.101.10/24 brd 172.16.101.255 scope global enp4s0f0
        valid lft forever preferred lft forever
    inet6 fe80::ec77:cb72:5eb9:4e29/64 scope link
        valid lft forever preferred lft forever
```

- OpenVswitch
 - 가상 스위치를 생성하여 물리 L3 스위치와 서버 간 연결 담당
 - Server1, Server2에 openVswitch 설치
 - ovs-vlan을 생성하여 격리된 환경에서의 VM 생성 가능
 - 서버1에는 VLAN30, VLAN40을 설정
 - 서버2에는 VLAN30, VLAN50을 설정
 - 가상 서버의 부하 분산 및 보안성 증진
- LACP
 - L3 Switch와 연결되어 있는 3개의 물리 포트에 LACP bonding 활성화시켜서 물리서버와 L3 Switch간의 통신확인

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

KVM생성 및 Snapshot (Server1, Server2)



- KVM생성
 - 서버1, 서버2에 KVM 설치 후
 - 서버1에 nginx서버 1대, db서버1대, php서버2대, vyos 1대, ESXi 1대 총 6대 가상머신 생성
 - 서버2에 nginx서버 1대, php서버2대, vyos 1대, ESXi 2대 총 6대 가상머신 생성
 - 서버 구축으로 격리된 환경에서 가상머신 생성하여 효율적으로 자원을 분배, 비용 절감 효과
- Snapshot
 - 스냅샷 CLI 방식으로 생성
 - 스냅샷 GUI 방식으로 생성
 - 설정 중의 오류가 발생했을 때 스냅샷 시점으로 서버 복구 가능

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

VyOS (Server1, Server2)

```

vyos on QEMU/KVM@server1
File Virtual Machine View Send Key

[10879.898397] vyos-config[2154]: Configuration success
[10879.939518] vyos-config[2167]: Configuration success

Welcome to VyOS - vyos1 tty1

vyos1 login: vyos
Password:
Welcome to VyOS!

Check out project news at https://blog.vyos.io
and feel free to report bugs at https://phabricator.vyos.net

You can change this banner using "set system login banner post-login" command.

VyOS is a free software distribution that includes multiple components,
you can check individual component licenses under /usr/share/doc/*/copyright
vyos@vyos1:~$ _

```

Interface	IP Address	S/L	Description
-----	-----	---	-----
eth0	192.168.101.11/24	u/u	
eth1	172.16.101.254/24	u/u	
eth2	172.16.102.254/24	u/u	
lo	127.0.0.1/8	u/u	
	::1/128		

- VyOS
 - Server1, Server2에 VyOS 1대를 vyos 이미지파일로 각각 KVM 가상 머신으로 설치
 - 3개의 가상 포트 eth0, eth1, eth2에 static으로 IP주소, 서브넷, 게이트웨이 등 설정
 - ovs-vlan 별로 가상머신 게이트웨이 설정

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

VyOS ospf (Server1, Server2)

```

vyos@vyos1:~$ sh ip ospf route
===== OSPF network routing table =====
N IA 10.0.0.0/8          [2] area: 0.0.0.0
                        via 192.168.101.251, eth0
N   172.16.101.0/24      [1] area: 0.0.0.10
                        directly attached to eth1
N   172.16.102.0/24      [1] area: 0.0.0.10
                        directly attached to eth2
N IA 172.16.103.0/24      [3] area: 0.0.0.0
                        via 192.168.101.251, eth0
N   192.168.100.0/24      [2] area: 0.0.0.0
                        via 192.168.101.251, eth0
N   192.168.101.0/24      [1] area: 0.0.0.0
                        directly attached to eth0
N   192.168.102.0/24      [2] area: 0.0.0.0
                        via 192.168.101.251, eth0

===== OSPF router routing table =====
R   192.168.100.1         [2] area: 0.0.0.0, ASBR
                        via 192.168.101.251, eth0
R   192.168.101.0         [2] area: 0.0.0.0, ABR
                        via 192.168.101.251, eth0
R   192.168.102.252       [1] area: 0.0.0.0, ABR
                        via 192.168.101.251, eth0

===== OSPF external routing table =====
N E2 0.0.0.0/0           [2/1] tag: 1
                        via 192.168.101.251, eth0

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.102.252	1	Full/DR	39.223s	192.168.101.251	eth0:192.168.101.11

Server 1 - VyOS

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.102.252	1	Full/DR	39.190s	192.168.102.252	eth0:192.168.102.21

Server 2 - VyOS

- VyOS ospf
 - 인터페이스 eth0는 backbone area 0 선언
 - 인터페이스 eth1, eth2는 area 10 선언
 - 선언한 결과로 Server1은 L3 Switch의 VLAN 10과 Neighbor을 맺음
 - Server2는 L3 Switch의 VLAN 20과 Neighbor을 맺음
 - 물리 서버들의 VLAN 가상 서버들을 Routing 통신을 하기 위해 설정
 - OSPF 라우팅 프로토콜로 인해 외부와 통신 가능

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

VxLAN (Virtual eXtention LAN) (Server1, Server2)

```

Port ovs0-vx30
tag: 30
Interface ovs0-vx30
type: vxlan
options: {key="30", remote_ip="192.168.102.20"}

```

Server 1

```

Port ovs0-vx30
tag: 30
Interface ovs0-vx30
type: vxlan
options: {key="30", remote_ip="192.168.101.10"}

```

Server 2

```

[root@Server2 ~]# ip route
default via 172.16.20.30 dev ovs0 proto static metric 803
default via 10.0.0.1 dev enp4s0f1 proto static metric 900

```

- VxLAN
 - Server1과 Server2에는 동일한 VLAN 30이 생성되어있는데 VLAN 30은 ESXi 가상머신의 네트워크로 지정
 - 두 물리 서버 사이의 VxLAN tunneling을 통해 VLAN 30 네트워크 대역의 가상 머신들이 서로 통신 가능하도록 설정
- 여기서 ovs0-if 대역 default-gateway metric을 낮게 조정해야 서로 통신 가능

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

NFS (Server1)

```
[root@server1 ~]# ls -l /web
total 2424204
drwxr-xr-x. 16 nginx nginx    4096 Aug 22 17:03
-rw-r--r--. 1 root  root    10709017 Aug 22 16:56
-rw-r--r--. 1 root  root      23 Aug 23 11:18
-rw-r--r--. 1 root  root      23 Aug 22 15:43
-rw-r--r--. 1 root  root      20 Aug 22 14:21
-rw-r--r--. 1 root  root    24269995 Aug 9 06:11
drwxr-xr-x. 2 root  root      4096 Aug 24 15:53
-rw-r--r--. 1 root  root    2447376384 Aug 23 18:06
drwxr-xr-x. 2 root  root      170 Aug 24 16:00
drwxr-xr-x. 2 root  root      170 Aug 24 16:02
drwxr-xr-x. 5 nginx nginx    4096 Aug 9 06:11
[root@server1 ~]# ssh root@nginx-1
Last login: Thu Aug 24 16:09:25 2023 from 172.16.102.10
[root@nginx-1 ~]# ls -l /usr/share/nginx/html/
total 2424204
drwxr-xr-x. 16 977 972    4096 Aug 22 17:03
-rw-r--r--. 1 root root    10709017 Aug 22 16:56
-rw-r--r--. 1 root root      23 Aug 23 11:18
-rw-r--r--. 1 root root      23 Aug 22 15:43
-rw-r--r--. 1 root root      20 Aug 22 14:21
-rw-r--r--. 1 root root    24269995 Aug 9 06:11
drwxr-xr-x. 2 root root      4096 Aug 24 15:53
-rw-r--r--. 1 root root    2447376384 Aug 23 18:06
drwxr-xr-x. 2 root root      170 Aug 24 16:00
drwxr-xr-x. 2 root root      170 Aug 24 16:02
drwxr-xr-x. 5 977 972    4096 Aug 9 06:11
[root@server1 ~]# cat /etc/exports
/web *(rw,no_root_squash,sync)
[root@nginx-1 ~]# showmount -e 192.168.101.10
Export list for 192.168.101.10:
/web *
```

• NFS

- Server1에 /web 위치에 공유 디렉터리 생성하여 3tier-web-architecture 가상 서버의 공유파일서버
 - nginx 가상 서버의 /usr/share/nginx/html 디렉터리를 mount 하여
- Server1의 /web 디렉터리와 nginx 가상 서버의 /html 디렉터리에 동일한 파일이 있음

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

DHCP (Server1)

```
[root@server1 ~]# cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#

#ovs0의 DHCP
dhcpd_interface = "ovs0";
subnet 192.168.101.0 netmask 255.255.255.0 {
    option routers 192.168.101.10;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 168.126.63.1;
    range dynamic-bootp 192.168.101.150 192.168.101.200;
    default-lease-time 3600;
    max-lease-time 7200;
    ##### pxe setting #####
    allow booting;
    allow bootp;
    next-server 192.168.101.10;
    filename "pxelinux.0";
}

#vlan30의 DHCP
dhcpd_interface = "vlan30";
subnet 172.16.101.0 netmask 255.255.255.0 {
    option routers 172.16.101.253;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 168.126.63.1;
    range dynamic-bootp 172.16.101.150 172.16.101.200;
    default-lease-time 3600;
    max-lease-time 7200;
    ##### pxe setting #####
    allow booting;
    allow bootp;
    next-server 192.168.101.10;
    filename "pxelinux.0";
}

#vlan40의 DHCP
dhcpd_interface = "vlan40";
subnet 172.16.102.0 netmask 255.255.255.0 {
    option routers 172.16.102.254;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 168.126.63.1;
    range dynamic-bootp 172.16.102.150 172.16.102.200;
    default-lease-time 3600;
    max-lease-time 7200;
    ##### pxe setting #####
    allow booting;
    allow bootp;
    next-server 192.168.101.10;
    filename "pxelinux.0";
}

#vlan50의 DHCP
dhcpd_interface = "vlan50";
subnet 172.16.103.0 netmask 255.255.255.0 {
    option routers 172.16.103.253;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 168.126.63.1;
    range dynamic-bootp 172.16.103.150 172.16.103.200;
    default-lease-time 3600;
    max-lease-time 7200;
    ##### pxe setting #####
    allow booting;
    allow bootp;
    next-server 192.168.101.10;
    filename "pxelinux.0";
}
```

- DHCP
 - Server 1에 DHCP 서버 설정
 - /etc/dhcp/dhcpd.conf에서 OVS와 각 VLAN의 IP 대역, 서브넷마스크, 게이트웨이를 각각 설정
 - 가상 머신에 인터페이스별 지정된 DHCP IP 대역을 할당하여 IP를 효율적으로 관리
 - 이를 통해 VLAN 별로 IP가 자동 할당된 가상 머신을 생성할 수 있어 편의성 증진

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

PXE & kickstart (Server1)

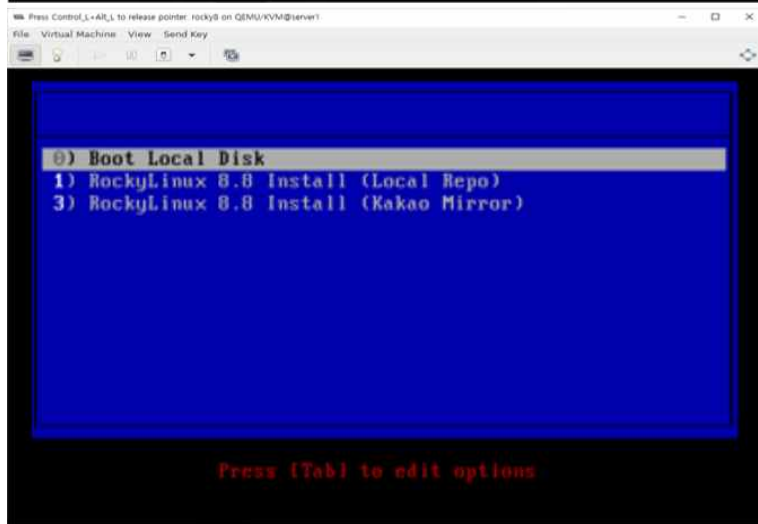
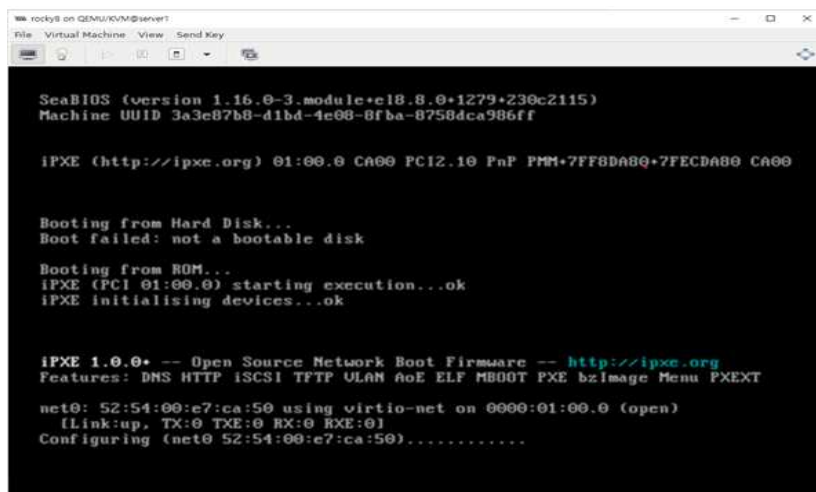
```
[root@server1 ~]# cat /var/lib/tftpboot/pxelinux.cfg/default
default menu.c32
prompt 0
timeout 150
ontimeout Rocky8

LABEL local
    MENU LABEL ^0) Boot Local Disk
    localboot 0

LABEL Rocky8
    MENU LABEL ^1) RockyLinux 8.8 Install (Local Repo)
    KERNEL /rocky8/vmlinuz
    APPEND initrd=/rocky8/initrd.img inst.repo=http://192.168.101.10/rocky8
    ks=http://192.168.101.10/rocky8/ks-rocky8.cfg

LABEL Rocky8-kakao
    MENU LABEL ^3) RockyLinux 8.8 Install (Kakao Mirror)
    KERNEL /rocky8/vmlinuz
    APPEND initrd=/rocky8/initrd.img inst.repo=https://mirror.kakao.com/linux/rocky/8.7/BaseOS/x86_64/os/ ks=http://192.168.101.10/rocky8/kakao-rocky8.cfg

[root@server1 ~]# ls -l /usr/share/nginx/html/rocky8/
total 2794092
-rw-r--r--. 1 root root      2306 Aug 25 02:41 kakao-rocky8.cfg
-rw-r--r--. 1 root root      2277 Aug 25 02:41 ks-rocky8.cfg
```



PXE & kickstart

- /var/lib/tftpboot/pxelinux.cfg/default에서 PXE-boot menu 편집하여 Local Repo 혹은 Kakao Mirror 사이트로 Rocky Linux 8.8 설치가 가능하게 함 (http를 통한 rocky linux설치)
- Kickstart 파일 생성 및 url을 기입하여 가상머신 생성시 OS 설치 및 Linux 기본설정 자동화

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

Nginx

```
[root@server1 ~]# dnf list installed | grep nginx
nginx.x86_64                               1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
nginx-all-modules.noarch                  1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
nginx-filesystem.noarch                   1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
nginx-mod-http-image-filter.x86_64        1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
nginx-mod-http-perl.x86_64                 1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
nginx-mod-http-xslt-filter.x86_64          1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
nginx-mod-mail.x86_64                     1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
nginx-mod-stream.x86_64                   1:1.22.1-1.module+el8.8.0+1272+5c2d9d1f
@appstream
```

```
[root@nginx-1 ~]# nginx -v
nginx version: nginx/1.22.1
```

- nginx
 - 서버1에 proxy 접속용으로 Nginx 1.22 버전 설치
 - nginx가 정적인 웹 콘텐츠를 제공하는데 사용하는 default 경로는 /usr/share/nginx/html

PHP

```
[root@php-1 ~]# php -v
PHP 8.2.9 (cli) (built: Aug 3 2023 11:39:08) (NTS gcc x86_64)
Copyright (c) The PHP Group
Zend Engine v4.2.9, Copyright (c) Zend Technologies
```

```
[root@php-2 ~]# php -v
PHP 7.4.33 (cli) (built: Aug 1 2023 08:47:49) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
```

```
[root@php-1 ~]# systemctl status php-fpm
● php-fpm.service - The PHP FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/systemd; vendor preset: enabled)
   Active: active (running) since Thu 2023-07-13 10:00:00 KST; 1min ago
     Main PID: 755 (php-fpm)
    Status: "Processes active: 0, idle: 6, Tasks: 7 (limit: 5922)"
   CGroup: /systemd/system/php-fpm.service
```

- php
 - 서버1,서버2에 version이 다른 PHP 가상 서버 2대 설치
 - /usr/share/nginx/html를 NFS 서버 /web과 mount함으로써
- nginx가상서버와 연동

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

DB

```

MariaDB-client.x86_64      10.6.15-1.el8      @mariadb
MariaDB-common.x86_64     10.6.15-1.el8      @mariadb
MariaDB-server.x86_64     10.6.15-1.el8      @mariadb
MariaDB-shared.x86_64     10.6.15-1.el8      @mariadb
galera-4.x86_64          26.4.14-1.el8      @mariadb

```

```

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| gnuboard |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.007 sec)

```

```

MariaDB [(none)]> select user,host,password from mysql.user;
+-----+-----+-----+
| User | Host | Password |
+-----+-----+-----+
| mariadb.sys | localhost | |
| root | localhost | *A4B6157319038724E3560894F7F932C8886EBFCF |
| mysql | localhost | invalid |
| gnuuser | localhost | *A4B6157319038724E3560894F7F932C8886EBFCF |
| gnuuser | % | *A4B6157319038724E3560894F7F932C8886EBFCF |
+-----+-----+-----+
5 rows in set (0.014 sec)

```

DB

- 데이터를 저장, 관리, 검색하기 위해 오픈소스 관계형 데이터베이스 관리 시스템인 mariaDB설치를 설치
- 웹서비스를 띄우기 위해 gnuboard에 대한 데이터베이스와 user생성

web proxy

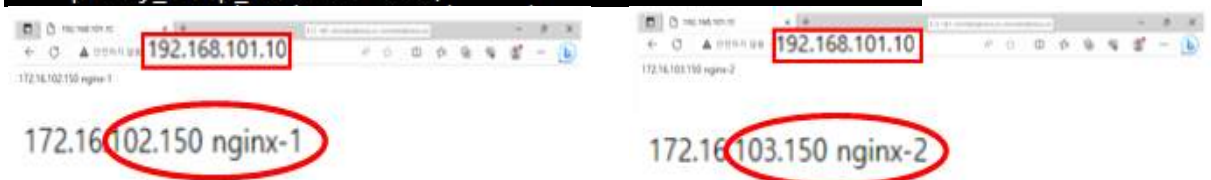
```

[root@server1 conf.d]# cat /etc/nginx/conf.d/proxy.conf
upstream web-proxy {
    server 172.16.102.150:80;
    server 172.16.103.150:80;
}

server {
    listen 80;
    server_name www.haknam.shop;

    location / {
        proxy_pass http://web-proxy;
        proxy_http_version 1.1;
    }
}

```



• web proxy

- /etc/nginx/conf.d/proxy.conf에서 로드밸런싱 설정하여 가용성 및 부하 분산시키고 백엔드 서버인 nginx-1, nginx-2의 IP주소를 감춰서 외부로부터 직접적인 접근을 제한하여 보안 강화

프로젝트 완료 보고서

프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

php proxy

The image displays two browser windows and a terminal window. The left browser window shows the PHP version 8.2.9 at the URL 192.168.101.10/info.php. The right browser window shows the PHP version 7.4.33 at the same URL. The terminal window shows the nginx configuration for the php proxy, with the stream section highlighted by a red box.

```

events {
    worker_connections 1024;
}

stream {
    upstream php-fpm {
        server 172.16.102.151:9000;
        server 172.16.102.152:9000;
    }

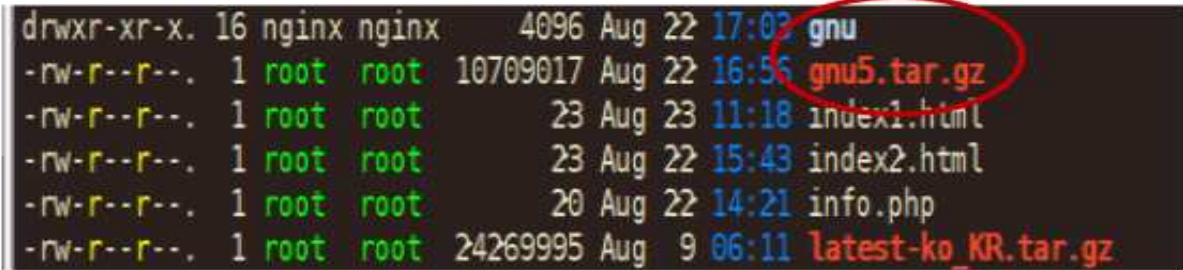
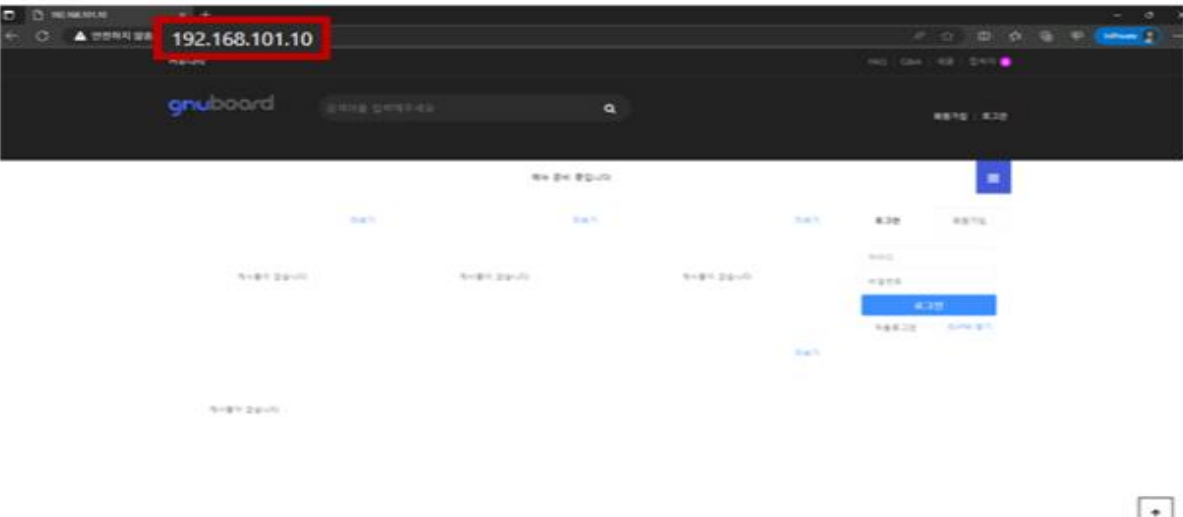
    server {
        listen 9000;
        proxy_pass php-fpm;
        proxy_timeout 3s;
        proxy_connect_timeout 1s;
    }
}

http {
    log_format main '$remote_addr
                    '$status $bod
                    '"$http_user
  
```

- php proxy
 - nginx-1 가상서버에서 php-1과 php-2 가상서버로 php proxy 접근 설정
 - php.conf 파일에서 백엔드 서버인 php-1,php-2의 IP와 port번호 작성
 - timeout을 3초로 설정하여 3초마다 다른 php가상서버로 접근하도록 설정
 - 로드밸런싱

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

gnuboard

- gnuboard
 - 오픈소스 기반의 웹 콘텐츠 관리 시스템으로 gnuboard선택
 - Server1, Server2에 설치된 nginx 가상서버에 웹 서버 테스트 용 gnuboard 설치 한 후 web proxy IP로 gnuboard 접속이 가능하게 함

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

GRE over IPsec (Server1, Server2)

```
vyos@vyos1:~$ sh int tunnel tun0
tun0@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
    link/gre 192.168.101.11 peer 192.168.102.21
    inet 10.10.10.1/30 brd 10.10.10.3 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::fc3a:7fff:fe10:a61d/64 scope link
        valid_lft forever preferred_lft forever

RX:  bytes  packets  errors  dropped  overrun    mcast
     0         0        0       0         0         0
TX:  bytes  packets  errors  dropped  carrier    collisions
     0         0        0       0         0         0
```

```
vyos@vyos1:~$ sh vpn ike sa
Peer ID / IP                               Local ID / IP
-----
192.168.102.21                             192.168.101.11

  State  IKEVer  Encrypt  Hash    D-H Group    NAT-T  A-Time  L-Time
  ----  -
  up      IKEv2   aes128   sha1_96  2(MODP_1024) no      3600    28800
```

```
vyos@vyos1:~$ show vpn ipsec sa
Connection      State  Uptime  Bytes In/Out  Packets In/Out  Remote address  Remote ID  Proposal
-----
peer-192.168.102.21-tunnel-1  up    3m47s   0B/0B        0/0            192.168.102.21  N/A       AES_CBC_128/HMAC_SHA1_96/MODP_1024
```

- GRE over IPsec
 - Server 1, Server 2에 설치된 VyOS1과 VyOS2에서 GRE over IPsec 설정으로 전용 가상 터널 인터페이스 tunnel 0 생성
 - tunnel 0에 IPsec을 추가로 설정 => 암호화 통신이 가능해짐(네트워크 보안성 확보)

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

DDNS(Dynamic Domain Name System) (Server1)

```

[root@server1 ~]# cat /usr/local/share/cloudflare-ddns.sh
#!/bin/bash

### dnf install bind-utils -y 를 해서 host command 설치 되어야 함
### cloudflare information
dns_record="haknam.shop"
zoneid="e0ba51668a62622fb32a81c3b72be13a"
cloudflare_zone_api_token="EkcxQ0txgBSy4aT08ofHNQBIRXIiXo1D5Br6h0GY"
proxied="false"
ttl=120

```

haknam.shop에 대한 DNS 관리
 DNS 레코드를 검토, 추가 및 편집합니다. 편집 내용이 저장되면 적용됩니다.

가져오기 및 내보내기 ▼

대시보드 디스플레이 설정

DNS 레코드 검색

▼ 필터 추가

유형	이름	콘텐츠	프록시 상태	TTL	작업
A	haknam.shop	175.197.24.178	DNS 전용	2분	편집
CNAME	www	haknam.shop	DNS 전용	자동	편집

API 토큰
 계정, 사이트 및 제품에 대한 액세스 및 권한을 관리합니다

토큰 생성

토큰 이름	권한	리소스	상태
haknam.shop	영역.DNS	1개 영역	활성

- DDNS
 - － 웹 서버의 IP가 바뀌더라도 해당 도메인만으로 변경된 IP로 찾아갈 수 있게 해주는 DDNS사용
 - － cloudflare를 통해 www.haknam.shop 도메인 가상 호스트를 생성하고 IP를 자동으로 할당받음
 - － web proxy서버가 있는 Server 1에 쉘 스크립트를 작성하여 DDNS실행
 - － KVM 가상머신 web-proxy(gnuboard) : server_name www.haknam.shop

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

Crontab (Server1)

```
[root@server1 ~]# crontab -l
#cloudflare-ddns
*/5 * * * * /usr/local/share/cloudflare-ddns.sh
@reboot /usr/local/share/cloudflare-ddns.sh

#bond
@reboot ovs-vsctl set port bond0 lacp=active
@reboot ovs-vsctl set port bond0 bond_mode=balance-tcp
```

- Crontab
 - 위 DDNS 쉘 스크립트 방식으로는 IP가 유동적으로 바뀔 때마다 쉘 스크립트를 수동으로 실행해야하는 단점이 있어서 보완하기 위해 crontab 사용
 - 5분마다 DDNS 쉘 스크립트를 실행하고, Server 1이 재부팅 시 쉘 스크립트 실행 및 LACP bonding설정을 자동으로 수행하게 함

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

Health_check (web proxy) (Server1)

```
[root@server1 ~]# cat health-check.sh
#!/bin/bash

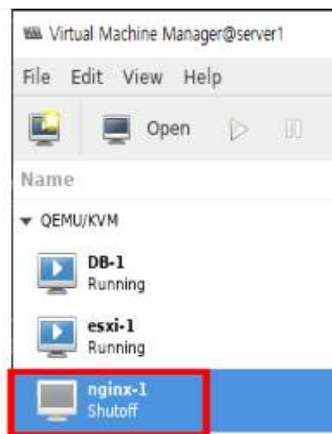
#curl, nc 설치 되어야 정상 가동
#curl은 web server health check, nc는 tcp health check에 사용
# 실행 시 백그라운드에서 실행되도록 shell script 이름 뒤에 & 붙여서 실행

while :
do
    #web health check 변수 지정 (0=success, 1=fail)
    web_status1=$(curl 172.16.102.150 --retry 3 --retry-max-time 3 -k -s -f -o /dev/null && echo "0" || echo "1")
    web_status2=$(curl 172.16.103.150 --retry 3 --retry-max-time 3 -k -s -f -o /dev/null && echo "0" || echo "1")

    #web server health check success/fail 시 nginx의 proxy 설정 편집
    if [ ${web_status1} -eq 0 ]
    then
        sed -i 's/#server 172.16.102.150/server 192.168.254.21/' /etc/nginx/conf.d/proxy.conf
    else
        sed -i 's/\ server 172.16.102.150/#server 192.168.254.21/' /etc/nginx/conf.d/proxy.conf
    fi

    if [ ${web_status2} -eq 0 ]
    then
        sed -i 's/#server 172.16.103.150/server 192.168.254.22/' /etc/nginx/conf.d/proxy.conf
    else
        sed -i 's/\ server 172.16.103.150/#server 192.168.254.22/' /etc/nginx/conf.d/proxy.conf
    fi

    #5초 기다린 후 while 무한 loop
    sleep 5
done
```



```
[root@server1 ~]# cat /etc/nginx/conf.d/proxy.conf
upstream web-proxy {
    #server 192.168.254.21:80;
    server 172.16.103.150:80;
}

server {
    listen 80;
```

- health_check(web proxy)
 - nginx proxy에는 health check 기능이 기본적으로 없으므로 web proxy가 있는 서버1에서 health check용 쉘 스크립트 작성
 - Server가 정상 작동하지 않을 경우 이를 확인하여 외부 사용자들이 해당 Server에 접근하지 못하도록 설정
 - 작동 여부는 **echo\$?** 명령어를 해당 서버에서 입력했을 때 결과값이 0이 나오면 정상 작동, 이외 다른 결과값이 나올 경우 해당 서버에 문제가 있음을 확인
 - 쉘 스크립트는 만약 웹 가상 서버 nginx-1, nginx-2 중 통신이 되지 않는 웹 서버가 감지되면 proxy.conf 파일에서 해당 웹 가상 서버 IP주소를 주석 처리함
 - 가용성 확보

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

health_check/php proxy) (Server1, Server2)

```
[root@nginx-1 ~]# cat php-health-check.sh
#!/bin/bash

#curl, nc 설치 되어야 정상 가동
#curl은 web server health check, nc는 tcp health check에 사용
# 실행 시 백그라운드에서 실행되도록 shell script 이름 뒤에 & 붙여서 실행

while :
do
    #php health check 변수 지정 (0=success, 1=fail)
    php_status1=$(nc -w 3 -v 172.16.102.151 9000 </dev/null >/dev/null 2>&1; echo $?)
    php_status2=$(nc -w 3 -v 172.16.102.152 9000 </dev/null >/dev/null 2>&1; echo $?)

    #php server health check success/fail 시 nginx의 proxy 설정 편집
    if [ ${php_status1} -eq 0 ]
    then
        sed -i 's/#server 172.16.102.151/server 172.16.102.151/' /etc/nginx/nginx.conf
    else
        sed -i 's/\ server 172.16.102.151/#server 172.16.102.151/' /etc/nginx/nginx.conf
    fi

    if [ ${php_status2} -eq 0 ]
    then
        sed -i 's/#server 172.16.102.152/server 172.16.102.152/' /etc/nginx/nginx.conf
    else
        sed -i 's/\ server 172.16.102.152/#server 172.16.102.152/' /etc/nginx/nginx.conf
    fi

    #5초 기다린 후 while 무한 loop
    sleep 5
done
```



```
[root@nginx-1 ~]# cat /etc/nginx/nginx.conf
# For more information on configuration, see:
#   * Official English Documentation: http://nginx.org/en/docs/
#   * Official Russian Documentation: http://nginx.org/ru/docs/

user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log notice;
pid /run/nginx.pid;

# Load dynamic modules. See /usr/share/doc/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

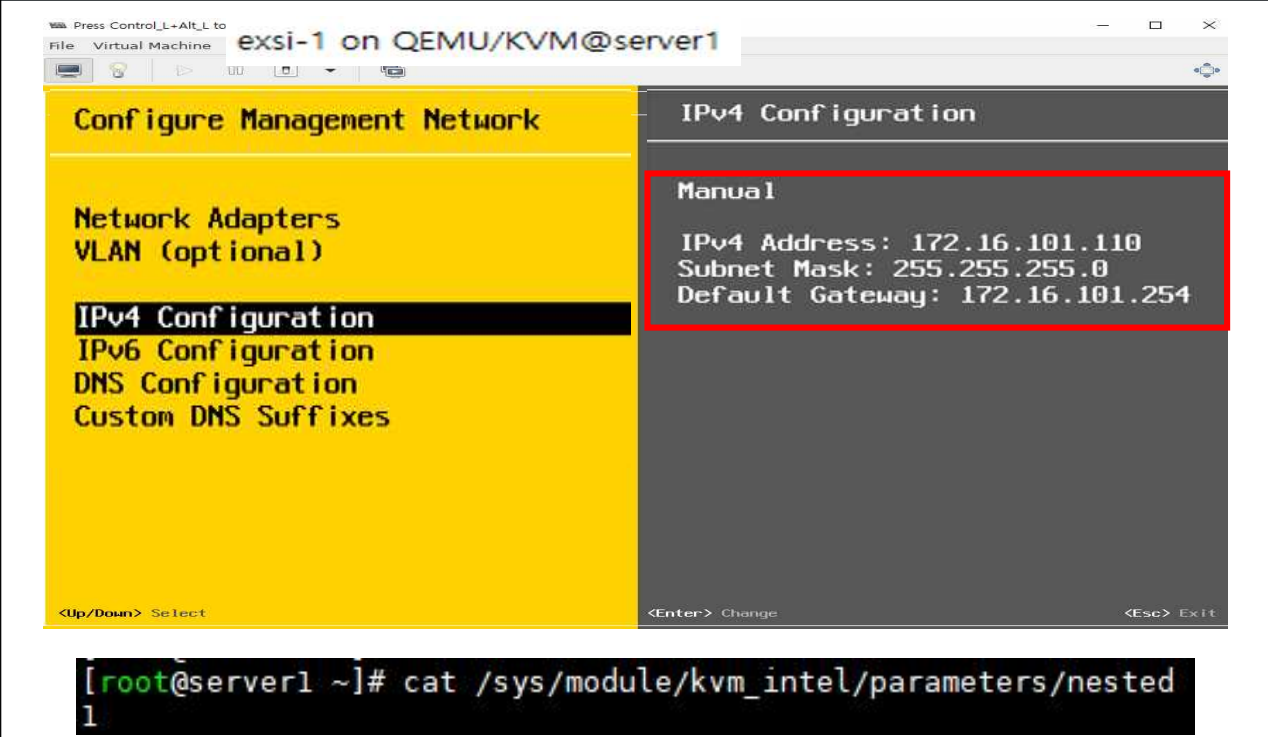
stream {
    #server 172.16.102.151:9000;
    server 172.16.102.152:9000;
```

• health_check/php proxy)

- nginx-1 가상서버에서 health_check 쉘 스크립트 생성
- 쉘 스크립트에는 nginx-1 가상 서버에서 php-1, php-2가상 서버 상태를 체크하는 명령어 있음
- 테스트 목적으로 Server 1의 php-1를 shutdown하였더니 nginx-1에서 php-1로 접근할 수 없음
- nginx.conf파일에서 php-1 IP와 포트가 주석 처리된 것을 확인
- php-1 가상 서버로는 요청을 전달하지 않음을 확인

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

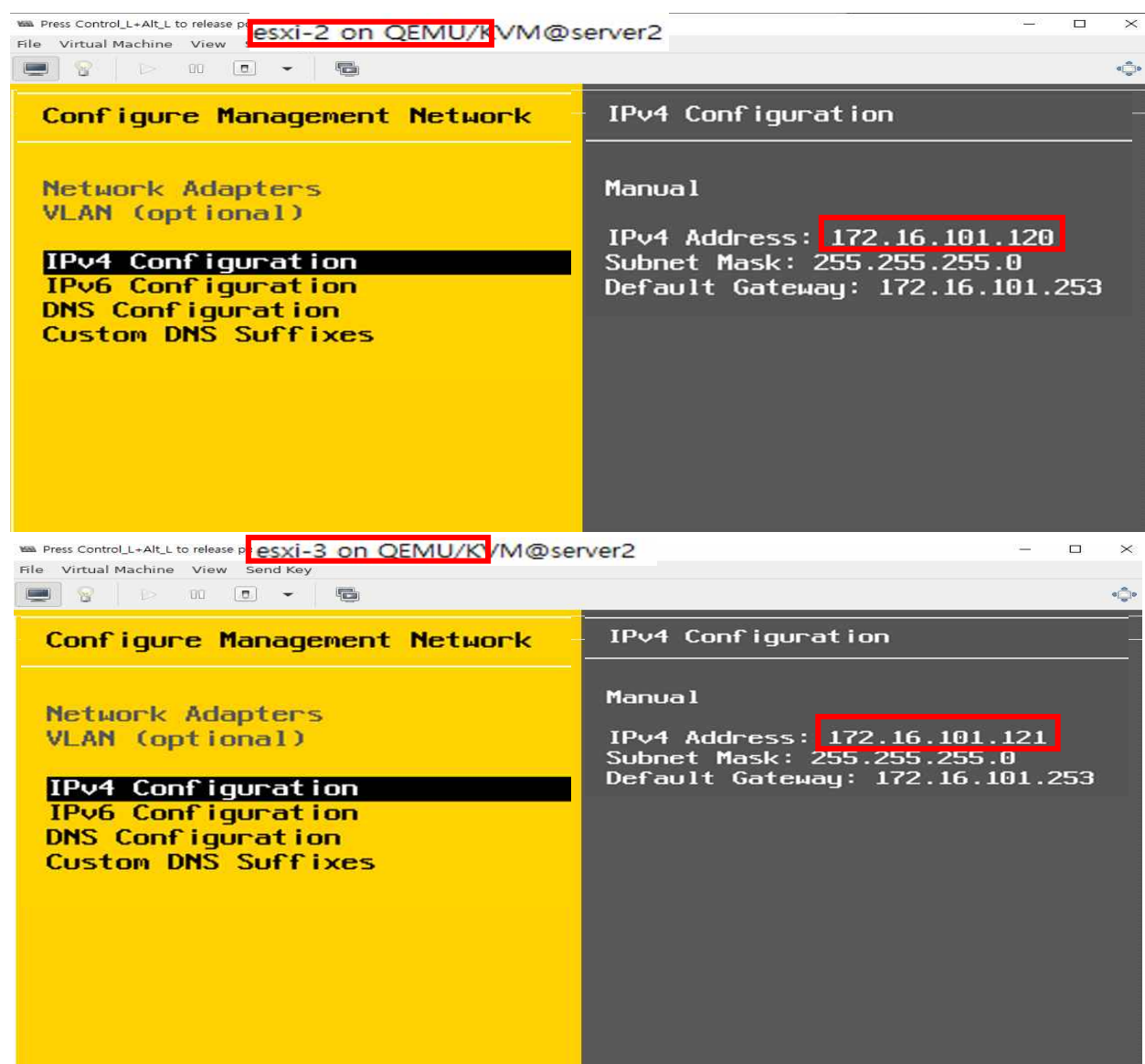
ESXi 설치 (Server1)



- Server1에 KVM으로 ESXi-1을 설치
- ESXi-1의 Static IP를 172.16.101.110(VLAN30대역)을 설정
- Gateway는 VLAN30의 VyOS-1인터페이스 eth1 IP인 172.16.101.254설정)
- 물리 Server1에 nested KVM설정을 적용시켜 ESXi 가상 머신 안에 또 가른 가상 머신을 생성하는 중첩 가상화 가능하도록 설정

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

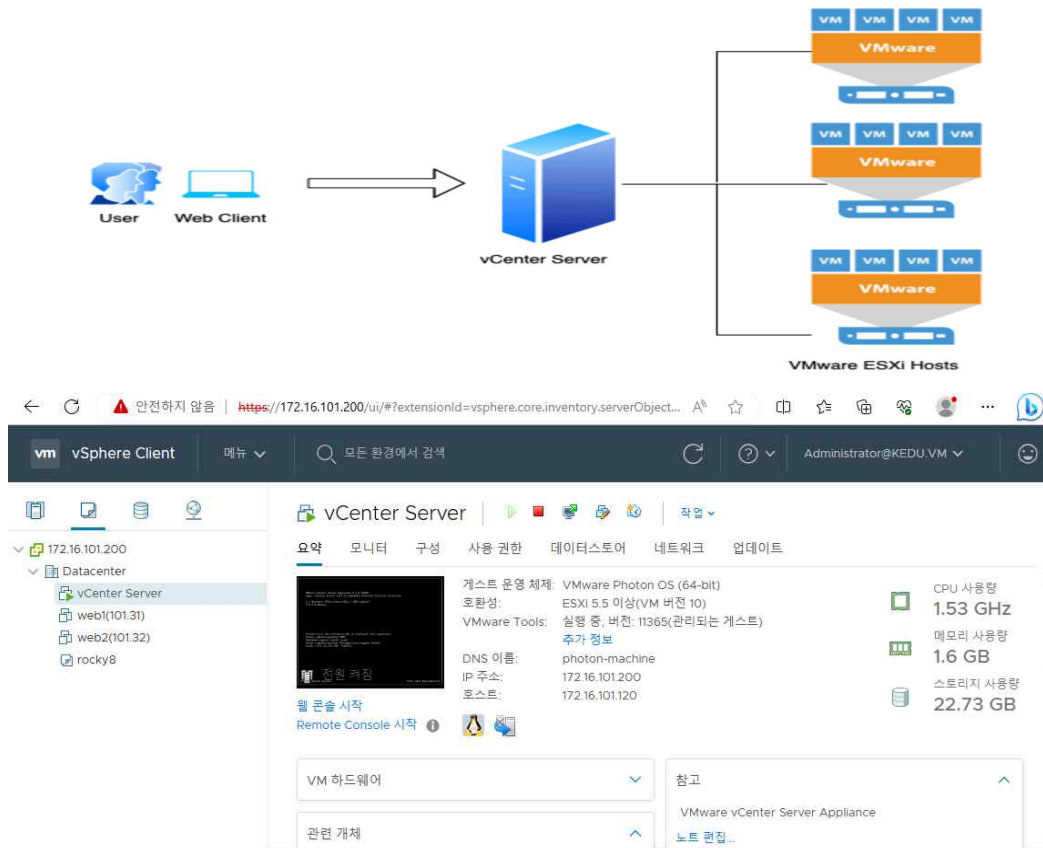
ESXi-2, ESXi-3 설치 (Server 2)



- Server2에 KVM으로 ESXi-2, ESXi-3을 설치
- ESXi-2의 Static IP를 172.16.101.120(VLAN30대역), ESXi-2의 Static IP를 172.16.101.121(VLAN30대역)
- Gateway는 VLAN30의 VyOS-2인터페이스 eth1 IP인 172.16.101.253설정
- 물리 Server2에 nested KVM설정을 적용시켜 ESXi 가상 머신 안에 또 가른 가상 머신을 생성하는 중첩 가상화 가능하도록 설정

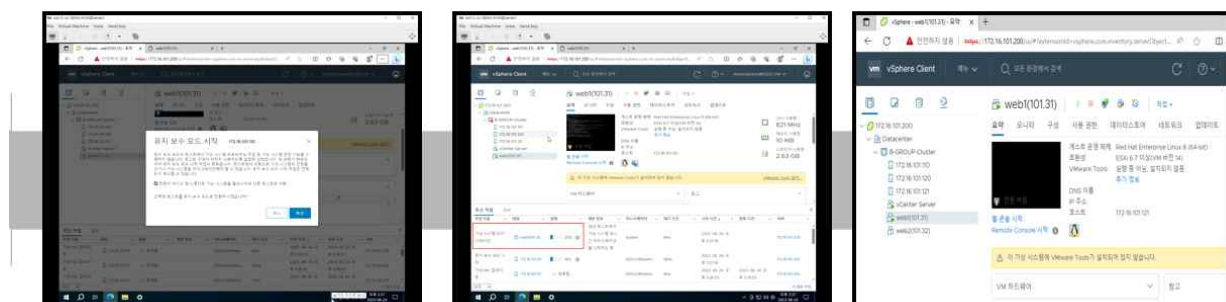
프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

VMware vCenter server (Server 1)



- ESXi-1를 호스트로 지정한 vCenter 가상 서버를 설치
- vCenter Server로 ESXi-1, ESXi-2, ESXi-3의 가상머신 관리 및 모니터링
- vCenter Server : 중앙집중화 관리, 리소스최적화, 가용성 및 복구관리, 성능 모니터링, 가상머신관리 보안 및 액세스 제어, 스토리지관리, 네트워크관리

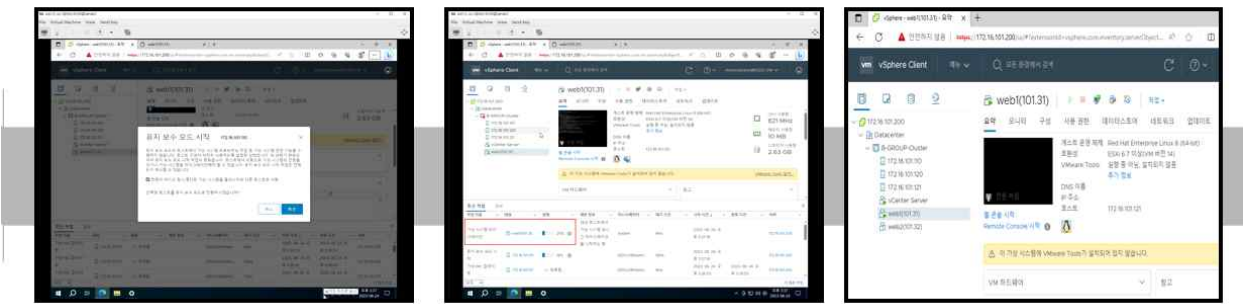
vCenter를 이용한 Migration



- 테스트 목적으로 ESXi-1에서 작동 중에 문제로 인해 VM을 사용없을 경우 ESXi-2, ESXi-3으로 잠깐 pause가 된 후 다시 작동 하면서 Migration이 되어 문제없이 VM이 다른 host에서 작동

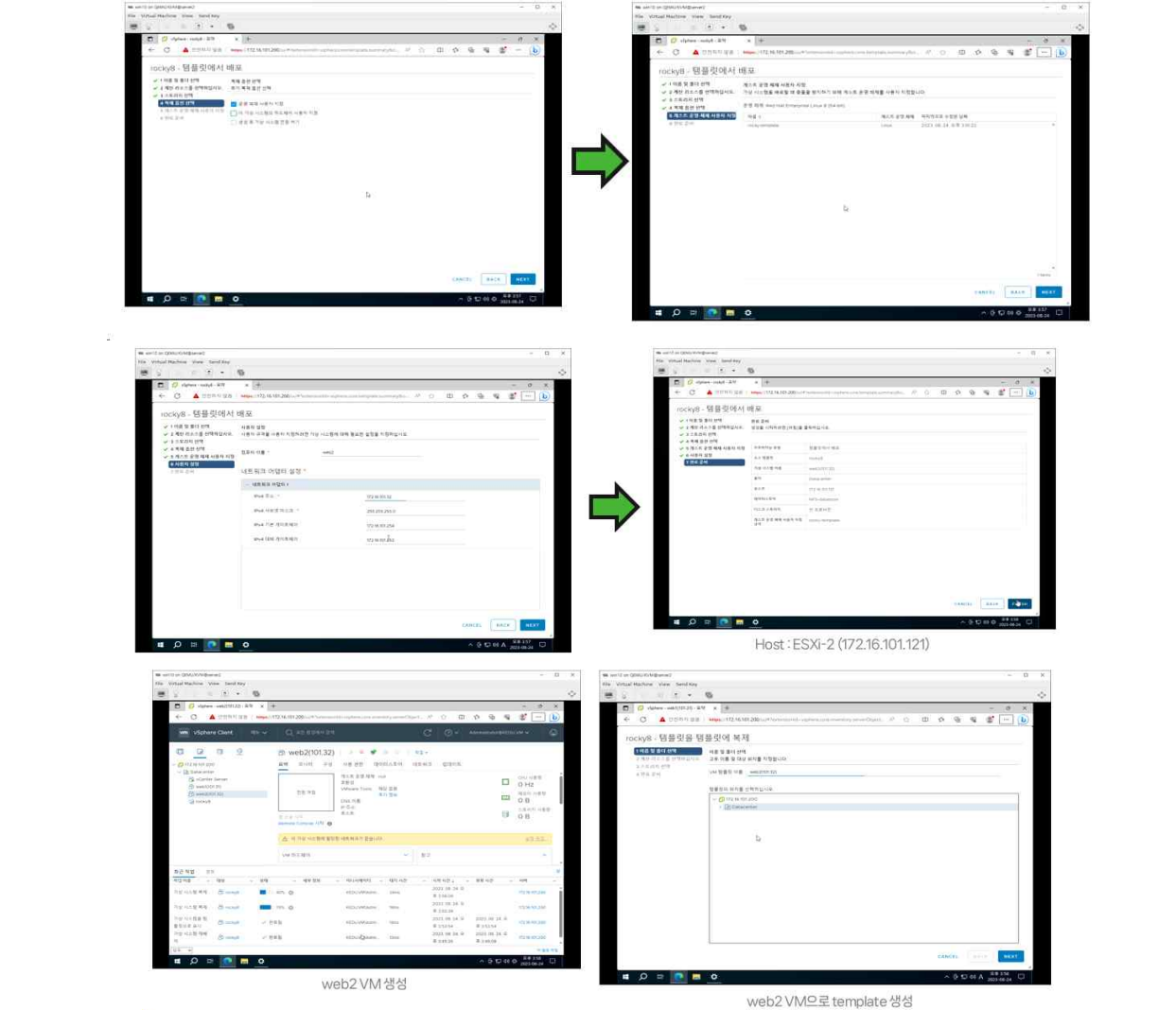
프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

Template을 이용한 VM 생성



- ESXi-1에서 작동 중에 문제로 인해 VM을 사용없을 경우 ESXi-2, ESXi-3으로 잠깐 pause가 된 후 다시 작동 하면서 Migration이 되어 문제없이 VM이 다른 host에서 작동

Template을 이용한 VM 생성



- Template을 이용한 VM생성
- VM 템플릿 선택 -> 템플릿을 VM으로 배포 -> 배포마법사 -> 구성설정 -> 네트워크구성 -> 배포시작 -> 완료 및 시작
- 편리하게 가상 머신들을 생성할 수 있음

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

(5) 구축 결과

가) 가상화를 구축하여 하나의 물리적 서버에서 여러 개의 가상 서버를 운영할 수 있습니다.

그로 인해 물리 장비의 자원 효율성, 확장성, 격리된 환경을 통한 운영에 대한 편의성 증대하였습니다.

나) Proxy 서버 구축으로 클라이언트가 실제 웹 서버에 직접 접속하지 않고도 Proxy 서버를 통해 웹 서비스를 이용하는 것이 가능해졌다. 이로 인해 실제 웹 서버의 대한 보안 강화, 개인 정보 보호, 캐싱 및 성능 최적화, 로드 밸런싱 등의 결과를 얻었습니다.

다) NAT, Port-forwarding, GRE over IPsec, Proxy 등의 설정을 통해서 포트와 서버 접근의 보안성이 향상되었습니다. 그로 인해 네트워크 트래픽 및 연결 관리, 내외부 통신, 트래픽 전달, 데이터 암호화의 이점을 얻었습니다.

라) 시스템 장애 시 자동복구 및 중단 없이 웹 서비스 제공이 가능해졌으며, Health-check와 vSphere 모니터링을 통해 신속한 대응이 가능해졌습니다.

프로젝트 완료 보고서																	
프로젝트 주제	KVM 가상 서버 구축 및 관리																
단계 : 프로젝트 완료	작성자 : 김학남									작성일 : 2023.07.12							

IV. 프로젝트 일정



프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

V. 시행착오

가. 물리 Server에 가상 머신을 생성하면서 디스크 용량을 확인하였더니 디스크 용량 분배를 수동으로 설정하지 않아서 /home 파티션에 대부분의 용량이 들어간 것을 보았습니다.

--> OS를 새로 설치한 후 디스크 수동 분배를 하였습니다.

- /boot : 1GB

- /swap : 10GB

- /root : 나머지

디스크 분배를 이렇게 나누어주면 다양한 요인에 기반하여 최적화된 시스템을 구성할 수 있었습니다.

/boot는 부팅과 관련된 파일들을 저장하는 파티션으로 1GB 정도의 공간으로 충분하였습니다.

/swap은 가상 메모리 또는 swap 공간을 제공하는 파티션으로 10GB 정도면 대부분의 시스템에서 충분한 점을 알게되었습니다.

그리고 /root에는 운영체제와 어플리케이션의 파일들이 저장되는 곳으로 남은 용량을 지정해 주었습니다.

나. 물리 Server를 재부팅 하였더니 네트워크와 연결되지 않는 문제가 발생하였습니다.

--> L3 Switch의 물리 서버와 연결되어 있는 LACP bonding이 Down 상태가 되어 있었습니다. 물리 Server 또한 마찬가지였습니다.

그리하여 물리 Server에 LACP bonding을 다시 설정해주었더니 네트워크 문제가 해결되었습니다.

이와 같은 문제를 방지하기 위해서 crontab을 이용하여 물리 Server를 재부팅 시 LACP를 자동으로 활성화하는 명령어를 적용시켰습니다.

이로 인해 다음에 서버를 재부팅하는 경우가 생기더라도 자동으로 LACP가 활성화 되도록 설정하여 수동으로 LACP 활성화 명령어를 입력할 필요가 없게 해결하였습니다.

프로젝트 완료 보고서		
프로젝트 주제	KVM 가상 서버 구축 및 관리	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.07.12

VI. 유지보수 계획

(1) 유지보수 개요

- 유지보수 방안 : 구축된 시스템의 유지관리를 위해 본 프로젝트 팀은 단계별 유지관리 계획을 유·무상 유지관리로 구분하고, 본 프로젝트 이후 안정화 단계를 거친 후 활용 및 개선 단계로 나누어 체계적인 관리가 되도록 다음과 같이 유지보수 방안을 수립한다.

(2) 유지보수 지원

2.1 무상 유지 보수 지원 :

- 무상유지보수 기간 : 검수 완료 후 한국정보교육원과 협의하여 정한 기간
- 무상유지보수 내역

지원분야	주요 지원 내용
시스템 안정화 지원	- 검수일로부터 1개월로 시스템 안정화를 위해 개발 및 구축에 참여한 실무 담당자 각 1명이 최소 1개월 이상 기술지원
원격점검 지원	- 원격 지원 시스템을 이용한 원격점검 지원
응급복구 지원	- 무상보수기간 동안 추가요청 사항이나 변경 사항이 발생할 경우 수정 보완 지원 - 시스템 장애가 발생한 경우 신고 후 4시간 이내 복구
유무선 지원	- 전화, Fax, 이메일 서비스 등 신속한 고객 응대를 통해 정확한 장애원인 판단 및 해결방안 제시 - Help Desk 운영

2.2 유상 유지 보수 지원 :

- 무상 보증기간 경과 후 1년 단위로 유지보수 계약을 체결한 경우에 한함
- 유상 유지보수 지원 내역은 무상 유지보수 지원 내역과 동일