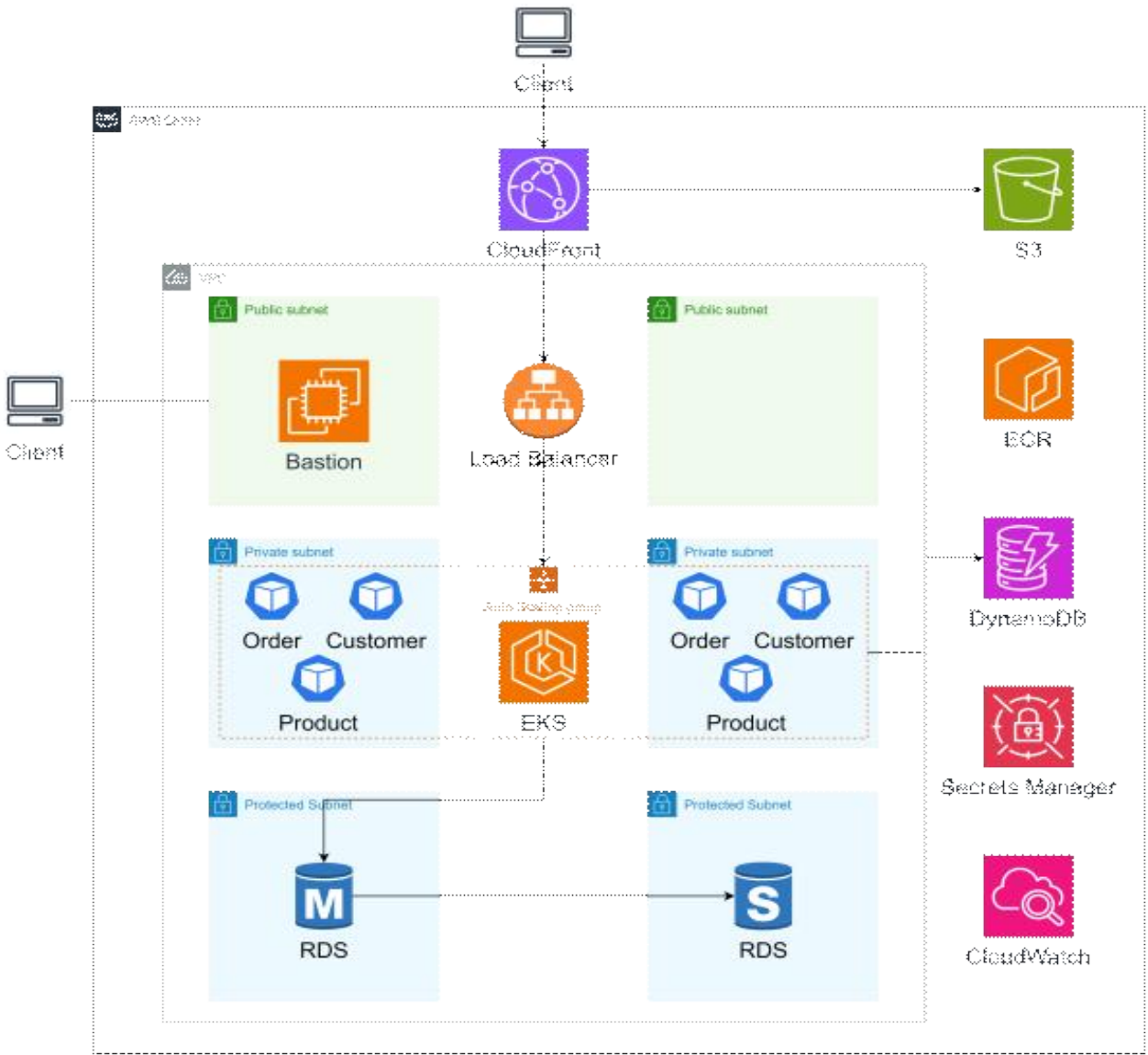
2024년도 전국기능경기대회

직 종 명	클라우드컴퓨팅	과 제 명	Solution architecture	과제번호	제 1과제
경기시간	4시간	비 번 호		심사위원 확 인	(인)

1. 요구사항

MSA(Micro Service Pattern)의 REST API를 포함하는 웹 서비스 환경을 구축하고 운영하고자 합니다. MSA 패턴의 REST API를 운영하는 데 있어 여러 장점이 있는 컨테이너 기반의 환경과 AWS 관리형 서비스인 EKS를 컨테이너 오케스트레이션 툴로 사용해야 합니다. 그 외에도 여러 가지 AWS 서비스를 사용하여 웹 서비스를 운영할 수 있는 클라우드 플랫폼을 구성해야 합니다. 주어진 아키텍처를 바탕으로 고가용성, 성능, 보안, 운영효율성 등 여러 가지 요소를 고려하여 웹 애플리케이션이 구동할 수 있는 클라우드 플랫폼을 구축해야 합니다.



Software Stack

AWS	개발언어/프레임워크
- VPC	- Golang
- EC2	- Docker
- EKS	
- ELB	
- ECR	
- CloudFront	
- S3	
- CloudWatch	
- RDS	
- DynamoDB	
- Secrets Manager	

2. 선수 유의사항

1) 기계 및 공구 등의 사용 시 안전에 유의하시고, 필요 시 안전장비 및 복장 등을 착용하여 사고를 예방하여 주시기 바랍니다.
2) 작업 중 화상, 감전, 찰과상 등 안전사고 예방에 유의하시고, 공구나 작업도구 사용 시 안전보호구 착용 등 안전수칙을 준수하시기 바랍니다.
3) 작업 중 공구의 사용에 주의하고, 안전수칙을 준수하여 사고를 예방하여 주시기 바랍니다.
4) 경기 시작 전 가벼운 스트레칭 등으로 긴장을 풀어주시고, 작업도구의 사용 시 안전에 주의하십시오.
5) 선수의 계정에는 비용의 제한이 존재하며, 이보다 더 높게 요금이 부과될 시 계정 사용이 불가능할 수 있습니다.
6) 문제에 제시된 괄호 박스 <>는 변수를 뜻함으로 선수가 적절히 변경하여 사용해야 합니다.
7) EC2 인스턴스의 TCP 80/443 outbound는 anyopen하여 사용할 수 있도록 합니다.
8) 과제의 Bastion 서버에서 대부분의 채점이 이루어짐으로 인스턴스를 생성하지 않았거나 종료된 상태면 채점이 불가능하니 각별히 주의하도록 합니다.
9) 과제 종료 시 진행 중인 테스트를 모두 종료하여 서버에 부하가 발생하지 않도록 합니다.
10) 별도 언급이 없는 경우, ap-northeast-2 리전에 리소스를 생성하도록 합니다.
11) 1페이지의 다이어그램은 구성을 추상적으로 표현한 그림으로, 세부적인 구성은 아래의 요구사항을 만족시킬 수 있도록 합니다. (ex. 서브넷이 2개 이상 존재할 수 있습니다.)
12) 모든 리소스의 이름, 태그, 변수과 변수는 대소문자를 구분합니다.
13) 문제에서 주어지지 않는 값들은 AWS Well-Architected Framework 6 pillars를 기준으로 적절한 값을 설정해야 합니다.
14) 배포 파일(html, Golang Binary) 수정 시 채점 전에 원래 상태로 되돌려야 합니다.
15) 불필요한 리소스를 생성한 경우, 감점의 요인이 될 수 있습니다. (e.g. VPC 추가 생성)

3. 네트워크 구성

클라우드 인프라에 대해 네트워크 레벨의 격리 및 분리가 가능하도록 아래 요구사항을 참고하여 VPC를 구성합니다. 서브넷 이름 뒤의 알파벳은 Availability Zone을 의미합니다. App Subnet에 속한 인스턴스(파드)들은 인터넷 액세스 없이 프라이빗하게 S3와 DynamoDB에 접근할 수 있어야 합니다. VPC의 네트워크 인터페이스로 들어오고 나가는 IP 트래픽에 대한 로그를 CloudWatch Logs에 기록해야 합니다.

VPC 정보

- VPC CIDR : 10.1.0.0/16
- VPC Tag : Name=wsi-vpc
- Internet G/W Tag : Name=wsi-igw
- Log Destination : /aws/vpc/wsi-vpc

App subnet A 정보

- CIDR : 10.1.0.0/24
- Tag : Name=wsi-app-a
- 외부 통신 : NAT G/W를 구성하여 인터넷 접근이 가능하도록 구성
- Route table Tag : Name=wsi-app-a-rt
- NAT G/W Tag : Name=wsi-natgw-a

App subnet B 정보

- CIDR : 10.1.1.0/24
- Tag : Name=wsi-app-b
- 외부 통신 : NAT G/W를 구성하여 인터넷 접근이 가능하도록 구성
- Route table Tag : Name=wsi-app-b-rt
- NAT G/W Tag : Name=wsi-natgw-b

Public subnet A 정보

- CIDR : 10.1.2.0/24
- Tag : Name=wsi-public-a
- 외부 통신 : Internet G/W를 구성하여 인터넷을 접근
- Route table Tag : Name=wsi-public-rt

Public subnet B 정보

- CIDR : 10.1.3.0/24
- Tag : Name=wsi-public-b
- 외부 통신 : Internet G/W를 구성하여 인터넷을 접근
- Route table Tag : Name=wsi-public-rt

Data subnet A 정보

- CIDR : 10.1.4.0/24
- Tag : Name=wsi-data-a
- 외부 통신 : 인터넷 접근이 필요하지 않음
- Route table Tag : Name=wsi-data-rt

Data subnet B 정보

- CIDR : 10.1.5.0/24
- Tag : Name=wsi-data-b
- 외부 통신 : 인터넷 접근이 필요하지 않음
- Route table Tag : Name=wsi-data-rt

4. Bastion Server

EC2를 활용해 Bastion 서버를 구성합니다. bastion 서버의 접근을 위해서 TCP 4272(SSH)를 사용합니다. Bastion 서버는 외부에서 SSH 프로토콜만을 허용하도록 Security Group을 구성합니다. Bastion 서버의 root는 kubernetes 내의 모든 리소스를 수정, 조회할 수 있는 권한이 미리 설정되어 있어야 합니다.

- Instance type : t3.small
- OS Image : Amazon Linux
- Subnet : Public subnet
- 설치 패키지 : AWS CLI v2, jq, curl, kubectl
- Tag : Name=wsi-bastion
- Security group name : wsi-bastion-sg (명시된 Security Group 하나만을 사용합니다.)
- EC2 IAM Role : 모든 리소스에 대해 full access를 가지는 role을 생성하여 붙입니다.
  Role의 이름은 wsi-bastion-role입니다.

5. NoSQL Database

order 애플리케이션의 데이터를 저장하기 위해서 NoSQL 데이터베이스인 DynamoDB를 구성합니다. order 애플리케이션 동작 설명을 기반으로 테이블을 설계하고 생성해야 합니다. Customer Managed Key로 암호화되어야 하며, 특정 시점으로 항상 복구할 수 있어야 합니다.

- Name : order
- Mode : On-demand

Table	Column	Data Type	ETC
order	id	String	Partition Key
	customerid	String	-
	productid	String	-

6. Relational Database

각 어플리케이션의 데이터를 저장하기 위해서 관계형 데이터베이스를 구성합니다. 고가용성을 보장해야 하고, 암호화와 백업 등을 활성화해야 합니다. 데이터베이스의 로그는 CloudWatch Logs로 모두 기록하도록 합니다. 보안을 위해 인터넷과 연결되지 않는 환경에 구성해야 하며 customer, product 애플리케이션만 접근할 수 있어야 합니다.
데이터베이스를 생성할 때 자격 증명을 Secrets Manager가 관리하도록 설정합니다. Secret Manager에 저장된 자격 증명 정보가 변경되면, 데이터베이스도 변경되어야 합니다.

- DB Cluster identifier : wsi-rds-mysql
- Instance class : db.m5.xlarge
- Engine Version : MySQL Community 8.0.35
- Port : 3306을 제외한 모든 포트
- Description of schema

Database	Table	Column	Data Type
wsi	customer	id	VARCHAR(255)
		name	VARCHAR(255)
		gender	VARCHAR(255)
	product	id	VARCHAR(255)
		name	VARCHAR(255)
		category	VARCHAR(255)

7. Web Application

customer, product, order 총 3개의 어플리케이션이 있습니다. 제공된 binary는 x86 기반 시스템에서 빌드하고 동작을 확인하였습니다.

- 모든 어플리케이션은 실행 시 TCP/8080 포트로 바인딩 됩니다.
- 모든 어플리케이션은 표준 출력으로 접근 로그를 출력합니다.
- 모든 어플리케이션은 /healthcheck 경로로 상태 확인을 제공합니다.
- 모든 어플리케이션은 환경변수를 통해 데이터베이스 연결 정보를 어플리케이션에 제공합니다. 환경변수 키 값은 각 애플리케이션의 설명을 참고합니다.

- customer

  customer 정보를 생성하고 제공하는 API 입니다. customer API는 Request body를 참조하여 데이터를 데이터베이스에 저장합니다.

  - API Spec

Path	Method	Request Format
/v1/customer	GET	Query String
		?id=xxxxxxx
/v1/customer	POST	Request Body
		'{"id":"xxxxxx","name":"xxxxxxx","gender":"xxxxxx"}'

  - OS Environment

Environment Key	Description
MYSQL_USER	RDBMS 연결에 사용할 사용자명
MYSQL_PASSWORD	RDBMS 연결에 사용할 사용자 암호
MYSQL_HOST	RDBMS 연결에 사용할 호스트 이름
MYSQL_PORT	RDBMS 연결에 사용할 포트번호
MYSQL_DBNAME	RDBMS 연결에 사용할 데이터베이스 이름

- product

  product 정보를 생성하고 제공하는 API입니다. product API는 Request body를 참조하여 데이터를 데이터베이스에 저장합니다.

  - API Spec

Path	Method	Request Format
/v1/product	GET	Query String
		?id=xxxxxxx
/v1/product	POST	Request Body
		'{"id":"xxxxxx","name":"xxxxxxx","category":"xxxxxx"}'

- OS Environment

Environment Key	Description
MYSQL_USER	RDBMS 연결에 사용할 사용자명
MYSQL_PASSWORD	RDBMS 연결에 사용할 사용자 암호
MYSQL_HOST	RDBMS 연결에 사용할 호스트 이름
MYSQL_PORT	RDBMS 연결에 사용할 포트번호
MYSQL_DBNAME	RDBMS 연결에 사용할 데이터베이스 이름

- order

order 정보를 생성하고 제공하는 API입니다. order API는 Request body를 참조하여 데이터를 데이터베이스에 저장합니다.

- API Spec

Path	Method	Request Format
/v1/order	GET	Query String
		?id=xxxxxxx
/v1/order	POST	Request Body
		'{"id":"xxxxxx","customerid":"xxxxxxx","productid":"xxxxxx"}'

- OS Environment

Environment Key	Description
AWS_REGION	DynamoDB 연결에 사용할 리전 코드 (e.g. ap-northeast-2)

8. Container Image Registry

AWS ECR를 사용해 애플리케이션의 컨테이너 이미지를 저장합니다. 모든 애플리케이션에 대해 각각 하나씩 레포지토리를 생성합니다. 세 레포지토리 모두 KMS 암호화와 취약점 분석 등이 가능해야 하며, 같은 태그를 가진 이미지가 업로드되지 않도록 구성합니다. 서울(ap-northeast-2) 리전 레포지토리로 이미지가 Push 되었을 때, 버지니아(us-east-1) 리전 레포지토리로 이미지가 복제되어야 합니다.

- customer 애플리케이션 레포지토리 이름 : customer
- product 애플리케이션 레포지토리 이름 : product
- order 애플리케이션 레포지토리 이름 : order

9. Container Orchestration

컨테이너 배포 및 관리를 효율적으로 수행하기 위해 오케스트레이션 툴을 사용합니다. Kubernetes의 Secret 리소스들은 반드시 KMS로 암호화해야 합니다. Private 형태의 EKS 클러스터를 생성하고, Kubernetes API는 외부에서 접근 불가능해야 하며, Bastion Server에서만 접근할 수 있어야 합니다. 모든 어플리케이션의 리소스들은 모두 wsi 라는 namespace에 존재해야 합니다. 호스트를 위한 EC2의 운영체제는 Kubernetes에 최적화된 운영체제인 Bottlerocket을 사용합니다. 노드 세트(EC2, Fargate)마다 각각 평상시에 2개 이상의 노드를 운용하여야 합니다.

- EKS Cluster name: wsi-eks-cluster
- Computing Type: EC2 (Managed Node Group)
- EKS version : 1.29
- EKS logging : Control plane 모두 5가지 로그가 저장되어야 함(API server, audit 등)

Addon Nodegroup

애플리케이션을 제외한 다른 모든 Addon들은 반드시 Addon Nodegroup에서 운용해야 합니다.

- Node group Name : wsi-addon-nodegroup
- Node EC2 Instance Tag : Name=wsi-addon-node
- Node EC2 Instance Type : t4g.large

App Nodegroup

customer, product 애플리케이션은 반드시 App Nodegroup에서 운용해야 하며, Addon의 DaemonSet Pod를 제외한 다른 리소스들을 App Nodegroup으로 운용해서는 안 됩니다.

- Node group Name : wsi-app-nodegroup
- Node EC2 Instance Tag : Name=wsi-app-node
- Node EC2 Instance Type : m5.xlarge

App Fargate

order 애플리케이션은 반드시 App Fargate에서 운용해야 하며, 그 외의 다른 리소스들은 App Fargate로 운용하면 안 됩니다.

- Fargate profile Name : wsi-app-fargate

Application Pod

App Nodegroup에 있는 Pod들은 EC2 Instance의 IAM 권한을 사용할 수 없게 해야 합니다. IAM 권한이 필요한 경우 Service Account 등을 이용해야 합니다. 또한, Secrets Manager에 있는 환경변수 정보는 Kubernetes Secret과 연동되어야 합니다. Secrets Manager에 있는 정보가 변경될 경우, 최대 2분 뒤에는 새로운 Pod에 새로운 환경변수가 적용되어야 합니다. Kubernetes Secret 값이 변경되었을 때 자동으로 Pod가 재시작되어야 합니다. 모든 애플리케이션 Pod는 높은 우선순위를 가져 쿠버네티스 내의 리소스가 부족해져도 우선적으로 종료되지 않아야 합니다.

- Secret Manager가 가지는 환경변수 : MYSQL_USER (username), MYSQL_PASSWORD (password)
- Required Package : curl
- Customer Pod/Deployment 이름 : customer
- Product Pod/Deployment 이름 : product
- Order Pod/Deployment 이름 : order

10. Load Balancer

ALB를 구성하여 외부에서 order, product, customer API에 각각 접근할 수 있도록 구성합니다. Security group을 이용하여 CloudFront를 통해서만 접근할 수 있도록 설정합니다. 기존 Pod가 종료되고 새로운 Pod가 나와도 정상적으로 서비스 할 수 있어야 합니다.

- Network facing : Internet-facing
- Listen : HTTP 80
- ALB Name : wsi-alb
- Tag : Name=wsi-alb

11. S3

S3를 통하여 정적 컨텐츠를 저장하고 제공합니다. S3의 모든 오브젝트는 CloudFront를 통해 외부 사용자들에게 제공될 수 있어야 하며, KMS로 암호화되어야 합니다. CloudFront 외에는 외부에서 접근하지 못하도록 구성합니다. 서울(ap-northeast-2) 리전 버킷으로 새로운 버전의 객체가 업로드됐을 때, 버지니아(us-east-1) 리전 버킷으로 객체가 복제되어야 합니다. Delete marker는 복제되지 않아야 합니다. 정적 배포 파일을 모두 업로드해야 하며, 추가적인 파일을 업로드해도 됩니다.

- 서울(ap-northeast-2) 리전 버킷 이름: ap-wsi-static-<임의의 4자리 영문>
- 미국(us-east-1) 리전 버킷 이름: us-wsi-static-<임의의 4자리 영문>

12. Cloud Front

CloudFront를 통하여 정적 컨텐츠 및 어플리케이션에 접근이 가능하도록 합니다. S3에 업로드 되는 정적 컨텐츠를 캐싱할 수 있도록 구성합니다. ALB로의 요청은 캐싱하지 않고, Query String도 모두 Origin으로 전달해야 합니다. 사용자가 CloudFront에 HTTP 접근 시에도 HTTPS로 리디렉션 되어 HTTPS로만 접근할 수 있도록 구성합니다. 또한, 서울(ap-northeast-2) 리전 버킷으로 접근 불가 시에 버지니아(us-east-1) 리전 버킷으로 접근할 수 있어야 합니다. 두 버킷 모두 접근 불가 시에는 503 에러 페이지가 나와야 합니다.

- Origin : S3와 ALB 두개의 origin을 가지도록 구성
- Edge : 한국뿐만 아니라 전 세계의 유저가 빠른 속도로 접근 가능하도록 구성
- Tag : Name=wsi-cdn
- 기타 : 채점 시 오동작 예방으로 IPv6는 비활성화하고, 하나의 CloudFront만 생성

13. Application Logging

Cloudwatch Logs를 통해 중앙 집중식 로깅 솔루션을 구성합니다. customer, product, order 각 어플리케이션에서 발생하는 접근 로그를 각 log group에 저장합니다. 다만 /healthcheck 경로에 대한 접근 로그는 Cloudwatch logs에 저장되지 않아야 합니다. 로그는 최대 1분 이내에 Cloudwatch Logs로 수집되어야 합니다.

- customer 어플리케이션 로그
  - 로그 그룹 이름 : /wsi/webapp/customer
- product 어플리케이션 로그
  - 로그 그룹 이름 : /wsi/webapp/product
- order 어플리케이션 로그
  - 로그 그룹 이름 : /wsi/webapp/order

14. Monitoring

CloudWatch의 Container Insights 기능을 이용하여 모니터링을 합니다. Container Insights 페이지에 접속했을 때 Cluster에 대한 정보(CPU, Memory, Nodes, Pods)를 한눈에 볼 수 있어야 합니다.

15. 지급재료 목록	직 종 명	클라우드컴퓨팅				
일련번호	재 료 명	규격(치수)	단위	1인당 소요량	공 동 소요량	비 고
1	AWS 계정	초기화 완료 및 리소스 생성 제한 없는 계정	개	3	3	선수x3 + 보조3
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						

16. 선수 지참재료 목록	직 종 명	클라우드컴퓨팅				
일련번호	재 료 명	규격(치수)	단위	1인당 소요량	공 동 소요량	비 고
1	키보드 및 마우스	유선	개	1	0	개인지참
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						

17. 경기장 시설목록

직 종 명	클라우드컴퓨팅

일련번호	시설 및 장비명	규격(치수)	단위	1인당 수량	공동수량	비 고
1	작업테이블	1200X600X720mm	대	1		선수용
2	의자	사무용 의자	대	1		선수용
3	전원	4구 멀티 콘센트 *전원용량: 선수수X1.0KW	개	1		
4	컴퓨터	CPU: 4Core 2GHz 이상 RAM: 16GB 이상 SSD: 200GB 이상 NIC: 1Gbps 이상 x 1 port GPU: 2개 이상 HDMI port Keyboard: USB type Mouse: USB type 광마우스	대	1	4	예비 4대
5	모니터	해상도 1920x1080	개	2	4	예비 4대
6	OS	Windows 10 Pro 이상	개	1		
7	Software	MS Office 2019 이상	개	1		
8	Software	Adobe Acrobat Reader	개	1		
9	Software	Visual Studio Code 최신	개	1		
10	Software	한글 2018 이상	개	1		
11	Software	Python 3.9.1 이상	개	1		
12	Software	OBS studio 30.1 이상	개	1		
13	Internet 회선	선수당 100Mbps 이상 보장 가능한 인터넷 회선	개	1	1	실 사용 1 백업 1
14	프린터	Color Laser 복합기 A4 양면 출력 가능	개	1		
15	라우터	Cisco ISR4321/K9 이상 (or 인터넷 성능 문제 없는 제품)	개	1		
16	스위치	Cisco WS-C2960S-48TS-L 상이 (or 인터넷 성능 문제 없는 제품)	개	1		
17	Network 시공	허브와 연결해 인터넷을 제공할 LAN cable	개	1		
18	컴퓨터	CPU: 4Core 2GHz 이상 RAM: 16GB 이상 SSD: 200GB 이상 키보드 마우스	개	10	0	심사용
19	테이블 및 공간	10명 심사위원이 앉을 수 있는 크기의 책상과 공간	개	0	1	심사용
20	스크린	65인치 이상 TV 혹은 빔프로젝터	개	0	1	공지용