

AWS

여행지기와 함께하는

클라우드 기술문서

2021. 11.



보다 더 나은 서비스

ESP B2 TEAM

Enhanced Services Partner

Project : 여행지기 VR VOD 제공 환경 구축

시나리오

회사 : ESP (Enhanced Service Partner)



클라이언트 : 여행지기 (Travel Friend)

- 관광객을 대상으로 가이드 투어와 패키지 상품을 제공하던 여행사
- 코로나로 인해 매출의 급격한 감소
- 새로운 상품 개발 (VR VOD Tour) & SNS EVENT 계획
- 문제점 발견

SNS 이벤트로 몰릴 트래픽을 대비할 인프라의 부재와 노후화된 장비

(인스타그램 기준 사이트 방문자 약 350% 증가의 홍보효과 발생)

- 아래의 요청사항과 함께 ESP에 VR VOD 제공 환경 구축을 의뢰

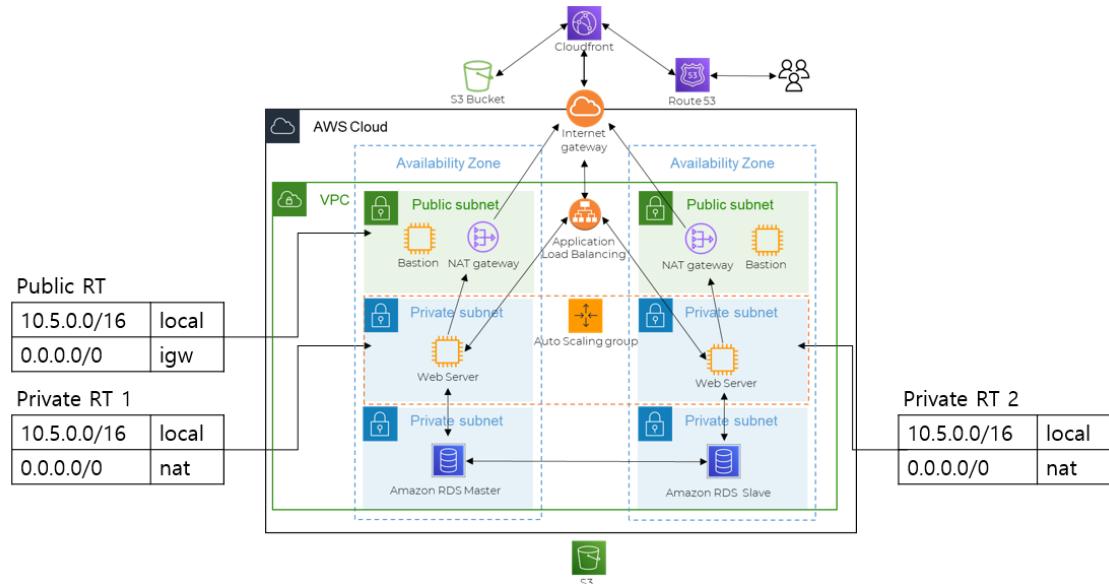
요청사항

- 1) AWS 마이그레이션
- 2) VOD Streaming 환경 구성
- 3) 향상된 인프라 (트래픽 제어)
- 4) 보안 & 백업 (고객의 중요 정보 보호)
- 5) 편리한 관리

ESP 솔루션

- 1) DMZ 서버를 기준 온프레미스 환경에서 AWS로 마이그레이션
- 2) Vedio On Demand를 통해 Streaming 환경 구성
- 3) LoadBalancing과 Auto Scaling을 통해 트래픽 제어
- 4) IAM, Security Group, S3, RDS를 통해 보안 및 백업 기능 강화
- 5) CloudWatch, Ansible, Zabbix를 통해 관리가 용이하게 구축

Project – 1. CloudFormation (TFUser)



- ✓ 가용영역 당 1개의 Public Subnet, 2개의 Private Subnet 생성
- ✓ Public Subnet에는 BastionHost와 NAT Gateway를 생성
- ✓ Private Subnet1,2에는 Web Server, Private Subnet3,4에는 RDS 생성
- ✓ Web Server 1,2는 Application LoadBalancing 및 Auto Scaling 설정
- ✓ RDS에 S3를 연결하여 고객의 정보를 안전하게 보관
- ✓ On Demand 서비스로 고객에게 VR VOD 제공

※ 전체적인 CloudFormation은 GitHub의 Travel_Friend User/Basic 파일 참고

1. CloudFormation (TFUser)

- 작업을 진행할 계정생성
- 계정에 작업권한을 부여

1) CloudFormation 작성

Project – 1. CloudFormation (TFUser)

```
{  
    "AWSTemplateFormatVersion": "2010-09-09",  
    "Description": "Travel_Friend_User",  
    "Resources": {  
        "TFUser": {  
            "Type": "AWS::IAM::User",  
            "Properties": {  
                "Path": "/",  
                "LoginProfile": {  
                    "Password": "P@$$w0rd"  
                },  
                "UserName": "TFUser"  
            }  
        },  
        "AdminPolicy": {  
            "Type": "AWS::IAM::Policy",  
            "Properties": {  
                "PolicyDocument": {  
                    "Version": "2012-10-17",  
                    "Statement": [  
                        {  
                            "Effect": "Allow",  
                            "Action": "*",  
                            "Resource": "*"  
                        }  
                    ]  
                },  
                "PolicyName": "Admin",  
                "Users": [  
                    {  
                        "Ref": "TFUser"  
                    }  
                ]  
            }  
        }  
    }  
}
```

=> User 생성
=> 계정 암호 설정
=> 계정 이름 설정
=> Policy 생성
=> Policy 지정
=> Policy를 부여할 계정 지정
3

Project – 1. CloudFormation (TFUser)

2) CloudFormation Upload

- CloudFormation 대쉬보드로 이동 후에 Create Stack 클릭
- Upload a template file 체크 후에 Choose file을 통해 파일 등록

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Template is ready Use a sample template Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL Upload a template file

Upload a template file
Choose file Travel_Friend%20User.json
JSON or YAML formatted file

S3 URL: https://s3.ap-northeast-2.amazonaws.com/cf-templates-5f8w8ac19yb6-ap-northeast-2/20213011Zs-Travel_Friend%20User.json [View in Designer](#)

Cancel **Next**

- Stack 이름 입력

Specify stack details

Stack name

Stack name
FTUser

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

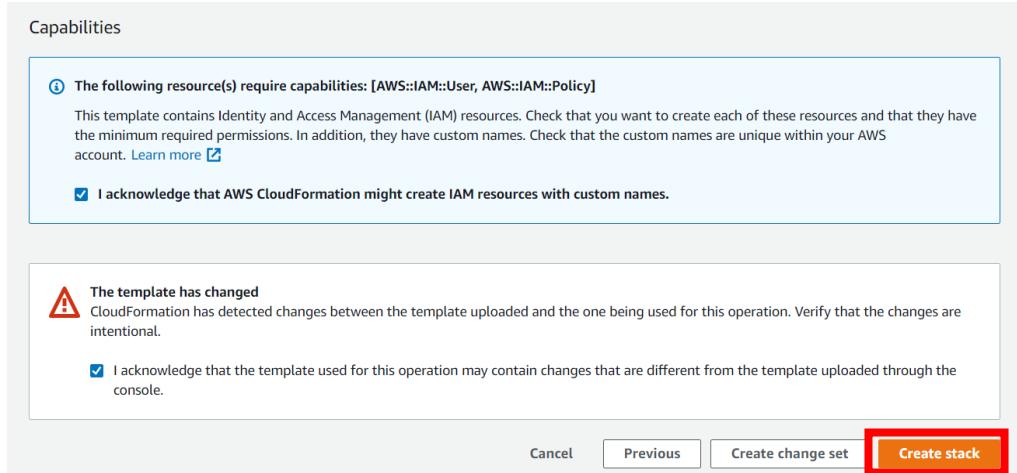
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters
There are no parameters defined in your template

Cancel Previous **Next**

Project – 1. CloudFormation (TFUser)

- Capabilities 체크 후 Create stack



- 생성 확인

Events (8)			
Timestamp	Logical ID	Status	Status reason
2021-10-28 17:44:40 UTC+0900	FTUser	CREATE_COMPLETE	-
2021-10-28 17:44:39 UTC+0900	AdminPolicy	CREATE_COMPLETE	-
2021-10-28 17:44:18 UTC+0900	AdminPolicy	CREATE_IN_PROGRESS	Resource creation Initiated
2021-10-28 17:44:16 UTC+0900	AdminPolicy	CREATE_IN_PROGRESS	-
2021-10-28 17:44:14 UTC+0900	FTUser	CREATE_COMPLETE	-
2021-10-28 17:43:58 UTC+0900	FTUser	CREATE_IN_PROGRESS	Resource creation Initiated
2021-10-28 17:43:37 UTC+0900	FTUser	CREATE_IN_PROGRESS	-
2021-10-28 17:43:34 UTC+0900	FTUser	CREATE_IN_PROGRESS	User Initiated

2. CloudFormation (TFBasic)

- FTUser 계정으로 로그인 한 후에 진행
- 기본 환경 구축 (VPC , Subnet , Instance , RDS)
- 전체적인 CloudFormation은 참고

1) Parameter

- AMI , IP Address , DB 정보
- 클라이언트(여행지기)가 원하는 값으로 변경 가능하도록 파라미터 설정
- 원하는 값이 없을 경우 Default 값으로 stack 생성

```
{  
    "AWSTemplateFormatVersion": "2010-09-09",  
    "Description": "Travel Friend Basic",  
    "Parameters": {  
        "AmazonLinuxAMIID": {  
            "Type": "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",  
            "Default": "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2"  
        },  
        "VPCCIDR": {  
            "Description": "CIDR Block for VPC",  
            "Type": "String",  
            "MinLength": "9",  
            "MaxLength": "18",  
            "Default": "10.5.0.0/16",  
            "AllowedPattern": "(\\d{1,3})\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}/(\\d{1,2})",  
            "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."  
        },  
        "PublicSubnet1Param": {  
            "Description": "Public Subnet 1",  
            "Type": "String",  
            "MinLength": "9",  
            "MaxLength": "18",  
            "Default": "10.5.10.0/24",  
            "AllowedPattern": "(\\d{1,3})\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}/(\\d{1,2})",  
            "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."  
        },  
        "PrivateSubnet1Param": {  
    }
```

=> CloudFormation의 정보

=> Instance 생성에 사용할 AMI 지정

=> VPC CIDR block 지정

=> Public Subnet1 CIDR

=> Private Subnet1 CIDR

Project – 2. CloudFormation (TFBasic)

```
"Description": "Private Subnet 1",
  "Type": "String",
  "MinLength": "9",
  "MaxLength": "18",
  "Default": "10.5.50.0/24",
  "AllowedPattern": "(\\W\\Wd{1,3})\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3})/(\\W\\Wd{1,2})",
  "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
},
"PrivateSubnet3Param": {                                     => Private Subnet3 CIDR
  "Description": "Private Subnet 3",
  "Type": "String",
  "MinLength": "9",
  "MaxLength": "18",
  "Default": "10.5.60.0/24",
  "AllowedPattern": "(\\W\\Wd{1,3})\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3})/(\\W\\Wd{1,2})",
  "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
},
"PublicSubnet2Param": {                                    => Public Subnet2 CIDR
  "Description": "Public Subnet 2",
  "Type": "String",
  "MinLength": "9",
  "MaxLength": "18",
  "Default": "10.5.20.0/24",
  "AllowedPattern": "(\\W\\Wd{1,3})\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3})/(\\W\\Wd{1,2})",
  "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
},
"PrivateSubnet2Param": {                                     => Private Subnet2 CIDR
  "Description": "Private Subnet 2",
  "Type": "String",
  "MinLength": "9",
  "MaxLength": "18",
  "Default": "10.5.100.0/24",
  "AllowedPattern": "(\\W\\Wd{1,3})\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3}\\W\\.\\W\\Wd{1,3})/(\\W\\Wd{1,2})",
  "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
```

Project – 2. CloudFormation (TFBasic)

```
},
"PrivateSubnet4Param": {                                     => Private Subnet4 CIDR
    "Description": "Private Subnet 4",
    "Type": "String",
    "MinLength": "9",
    "MaxLength": "18",
    "Default": "10.5.110.0/24",
    "AllowedPattern": "(WWd{1,3})WW.(WWd{1,3})WW.(WWd{1,3})WW.(WWd{1,3})/(WWd{1,2})",
    "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
},
"KeyName": {                                              => KeyPair 설정
    "Description": "Name of an existing EC2 KeyPair to enable SSH access to the
instance",
    "Type": "AWS::EC2::KeyPair::KeyName",
    "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
},
"DBName": {                                              => RDS DB 이름 설정
    "Default": "RDSDatabase",
    "Description": "The database name",
    "Type": "String",
    "MinLength": "1",
    "MaxLength": "64",
    "AllowedPattern": "[a-zA-Z] [a-zA-Z0-9]*",
    "ConstraintDescription": "must begin with a letter and contain only alphanumeric
characters."
},
"DBUser": {                                              => DB User 이름 설정
    "NoEcho": "true",
    "Description": "The database admin account username",
    "Type": "String",
    "MinLength": "1",
    "MaxLength": "16",
    "AllowedPattern": "[a-zA-Z] [a-zA-Z0-9]*",
    "ConstraintDescription": "must begin with a letter and contain only alphanumeric
characters."
},
"DBPassword": {                                         => DB Password 설정
    },
}
```

Project – 2. CloudFormation (TFBasic)

```
"NoEcho": "true",
"Description" : "The database admin account password",
"Type": "String",
"MinLength": "1",
"MaxLength": "41",
"AllowedPattern" : "[a-zA-Z0-9]+",
"ConstraintDescription" : "must contain only alphanumeric characters."
},
"DBAllocatedStorage": {                                     => DB 용량 설정
    "Default": "5",
    "Description" : "The size of the database (Gb)",
    "Type": "Number",
    "MinValue": "5",
    "MaxValue": "1024",
    "ConstraintDescription" : "ust be between 5 and 1024Gb."
},
"DBInstanceClass": {                                     => DB Instance Type 지정
    "Description" : "The database instance type",
    "Type": "String",
    "Default": "db.t2.micro",
    "AllowedValues" : [ "db.t1.micro", "db.m1.small", "db.m1.medium", "db.m1.large",
"db.m1.xlarge", "db.m2.xlarge", "db.m2.2xlarge", "db.m2.4xlarge", "db.m3.medium",
"db.m3.large", "db.m3.xlarge", "db.m3.2xlarge", "db.m4.large", "db.m4.xlarge",
"db.m4.2xlarge", "db.m4.4xlarge", "db.m4.10xlarge", "db.r3.large", "db.r3.xlarge",
"db.r3.2xlarge", "db.r3.4xlarge", "db.r3.8xlarge", "db.m2.xlarge", "db.m2.2xlarge",
"db.m2.4xlarge", "db.cr1.8xlarge", "db.t2.micro", "db.t2.small", "db.t2.medium", "db.t2.large"]
},
"ConstraintDescription" : "must select a valid database instance type."
},
"EC2SecurityGroup": {                                     => DB Instance Security Group
    "Description" : "The EC2 security group that contains instances that need access
to the database",
    "Default": "default",
    "Type": "String",
    "AllowedPattern" : "[a-zA-Z0-9WW-]+",
    "ConstraintDescription" : "must be a valid security group name."
},
"MultiAZ" : {                                         => MultiAZ 사용 여부
```

Project – 2. CloudFormation (TFBasic)

```
"Description" : "Multi-AZ master database",
  "Type" : "String",
  "Default" : "false",
  "AllowedValues" : [ "true", "false" ],
  "ConstraintDescription" : "must be true or false."
}
},
"Conditions": {
  "Is-EC2-VPC" : { "Fn::Or" : [ {"Fn::Equals" : [{"Ref" : "AWS::Region"}, "eu-central-1"]}, {"Fn::Equals" : [{"Ref" : "AWS::Region"}, "ap-northeast-2"]}]},
  "Is-EC2-Classic" : { "Fn::Not" : [{ "Condition" : "Is-EC2-VPC"}]}
},
```

2) Resources – VPC

```
"Resources": {
  "VPC": {
    "Type": "AWS::EC2::VPC",           => VPC 생성
    "Properties": {
      "CidrBlock": {
        "Ref": "VPCCIDR"            => Parameter에서 지정한 주소
      },
      "EnableDnsSupport": true,
      "EnableDnsHostnames": true,
      "Tags": [
        {
          "Key": "VPC",
          "Value": "NAT-and-CLI"
        },
        {
          "Key": "Name",
          "Value": "FT VPC"
        }
      ]
    }
  }
}
```

Project – 2. CloudFormation (TFBasic)

```
        ],
    }
},
```

3) Resources – InternetGateway & Attach

```
"InternetGateway": {
    "Type": "AWS::EC2::InternetGateway",
    "DependsOn": "VPC"
},
"AttachGateway": {
    "Type": "AWS::EC2::VPCGatewayAttachment",
    "DependsOn": [
        "VPC",
        "InternetGateway"
    ],
    "Properties": {
        "VpcId": {
            "Ref": "VPC"
        },
        "InternetGatewayId": {
            "Ref": "InternetGateway"
        }
    }
},
```

=> InternetGateway 이름
=> InternetGateway 생성
=> Attachment 이름
=> Attachment 생성
=> Attachment 할 VPC
=> Attachment 할 IGW

4) Resources – EIP & NAT Gateway

```
"EIP": {
    "Type": "AWS::EC2::EIP"
},
"EIP2": {
    "Type": "AWS::EC2::EIP"
},
```

=> EIP 이름
=> EIP 생성

Project – 2. CloudFormation (TFBasic)

```
"NATGateway" : {                                     => 생성할 NAT Gateway 이름  
    "Type": "AWS::EC2::NatGateway",                 => NAT Gateway 생성  
    "DependsOn": "AttachGateway",  
    "Properties": {  
        "AllocationId": { "Fn::GetAtt" : ["EIP", "AllocationId"]},   => EIP  
        "SubnetId": {  
            "Ref": "PublicSubnet1"                                => Subnet 위치 지정  
        }  
    }  
,  
"NATGateway2" : {  
    "Type": "AWS::EC2::NatGateway",  
    "DependsOn": "AttachGateway",  
    "Properties": {  
        "AllocationId": { "Fn::GetAtt" : ["EIP2", "AllocationId"]},  
        "SubnetId": {  
            "Ref": "PublicSubnet2"                                => Subnet 위치 지정  
        }  
    }  
,
```

5) Resources – Subnet (Public Subnet 1,2)

```
"PublicSubnet1": {                                     => 생성할 Subnet 이름  
    "Type": "AWS::EC2::Subnet",                      => Subnet 생성  
    "DependsOn": "AttachGateway",  
    "Properties": {  
        "VpcId": {  
            "Ref": "VPC"                                    => VPC 지정  
        },  
        "CidrBlock": {  
            "Ref": "PublicSubnet1Param"                  => Parameter에서 지정한 주소  
        },  
        "MapPublicIpOnLaunch": true,  
        "AvailabilityZone": {  
    }
```

Project – 2. CloudFormation (TFBasic)

```
"Fn::Select": [
    "0",
    {
        "Fn::GetAZs": {
            "Ref": "AWS::Region"
        }
    }
],
},
"Tags": [
    {
        "Key": "Name",
        "Value": "Public Subnet 1"
    }
]
},
"PublicSubnet2": {
    "Type": "AWS::EC2::Subnet",
    "DependsOn": "AttachGateway",
    "Properties": {
        "VpcId": {
            "Ref": "VPC"
        },
        "CidrBlock": {
            "Ref": "PublicSubnet2Param"
        },
        "MapPublicIpOnLaunch": true,
        "AvailabilityZone": {
            "Fn::Select": [
                "2",
                {
                    "Fn::GetAZs": {
                        "Ref": "AWS::Region"
                    }
                }
            ]
        },
    }
},
```

=> 가용영역 지정 (a)

=> 가용영역 지정 (c)

Project – 2. CloudFormation (TFBasic)

```
"Tags": [  
    {  
        "Key": "Name",  
        "Value": "Public Subnet 2"  
    }  
],  
},
```

6) Resources – Subnet (Private Subnet 1,2,3,4)

```
"PrivateSubnet1": {  
    "Type": "AWS::EC2::Subnet",  
    "DependsOn": "AttachGateway",  
    "Properties": {  
        "VpcId": {  
            "Ref": "VPC"  
        },  
        "CidrBlock": {  
            "Ref": "PrivateSubnet1Param"  
        },  
        "AvailabilityZone": {  
            "Fn::Select": [  
                "0",  
                {  
                    "Fn::GetAZs": {  
                        "Ref": "AWS::Region"  
                    }  
                }  
            ]  
        },  
        "Tags": [  
            {  
                "Key": "Name",  
                "Value": "Private Subnet 1"  
            }  
        ]  
    }  
},
```

Project – 2. CloudFormation (TFBasic)

```
        }
    ]
}
},
"PrivateSubnet3": {
    "Type": "AWS::EC2::Subnet",
    "DependsOn": "AttachGateway",
    "Properties": {
        "VpcId": {
            "Ref": "VPC"
        },
        "CidrBlock": {
            "Ref": "PrivateSubnet3Param"
        },
        "AvailabilityZone": {
            "Fn::Select": [
                "0",
                {
                    "Fn::GetAZs": {
                        "Ref": "AWS::Region"
                    }
                }
            ]
        },
        "Tags": [
            {
                "Key": "Name",
                "Value": "Private Subnet 3"
            }
        ]
    }
},
"PrivateSubnet2": {
    "Type": "AWS::EC2::Subnet",
    "DependsOn": "AttachGateway",
    "Properties": {
        "VpcId": {
            "Ref": "VPC"
        }
    }
},
```

Project – 2. CloudFormation (TFBasic)

```
        },
        "CidrBlock": {
            "Ref": "PrivateSubnet2Param"
        },
        "AvailabilityZone": {
            "Fn::Select": [
                "2",
                {
                    "Fn::GetAZs": {
                        "Ref": "AWS::Region"
                    }
                }
            ]
        },
        "Tags": [
            {
                "Key": "Name",
                "Value": "Private Subnet 2"
            }
        ]
    },
    "PrivateSubnet4": {
        "Type": "AWS::EC2::Subnet",
        "DependsOn": "AttachGateway",
        "Properties": {
            "VpcId": {
                "Ref": "VPC"
            },
            "CidrBlock": {
                "Ref": "PrivateSubnet4Param"
            },
            "AvailabilityZone": {
                "Fn::Select": [
                    "2",
                    {
                        "Fn::GetAZs": {
                            "Ref": "AWS::Region"
                        }
                    }
                ]
            }
        }
    }
},
```

Project – 2. CloudFormation (TFBasic)

```
        }
    }
]
},
"Tags": [
    {
        "Key": "Name",
        "Value": "Private Subnet 4"
    }
]
},
},
```

7) Resources – RouteTable & Route & Association (Public)

- Public Subnet 1,2 와 Internet Gateway

```
"PublicRouteTable": {
    "Type": "AWS::EC2::RouteTable",
    "DependsOn": [
        "VPC",
        "AttachGateway"
    ],
    "Properties": {
        "VpcId": {
            "Ref": "VPC"
        },
        "Tags": [
            {
                "Key": "Name",
                "Value": "Public"
            }
        ]
    }
},
"PublicRoute": {
```

=> Route Table 이름
=> Route Table 생성
=> VPC 지정
=> Route 이름

Project – 2. CloudFormation (TFBasic)

```
"Type": "AWS::EC2::Route",           => Route 생성
"DependsOn": [
    "PublicRouteTable",
    "AttachGateway"
],
"Properties": {
    "RouteTableId": {
        "Ref": "PublicRouteTable"      => Route Table 지정
    },
    "DestinationCidrBlock": "0.0.0.0/0",   => 목적지 CIDR 지정
    "GatewayId": {
        "Ref": "InternetGateway"     => Gateway 지정
    }
},
"PublicSubnet1RouteTableAssociation": {           => Association 이름
    "Type": "AWS::EC2::SubnetRouteTableAssociation",   => Association
    "DependsOn": [
        "PublicRouteTable",
        "PublicSubnet1",
        "AttachGateway"
    ],
    "Properties": {
        "SubnetId": {
            "Ref": "PublicSubnet1"      => Association할 Subnet 지정
        },
        "RouteTableId": {
            "Ref": "PublicRouteTable"   => Association할 RouteTable
        }
    }
},
"PublicSubnet2RouteTableAssociation": {
    "Type": "AWS::EC2::SubnetRouteTableAssociation",
    "DependsOn": [
        "PublicRouteTable",
        "PublicSubnet2",
        "AttachGateway"
    ],
}
```

Project – 2. CloudFormation (TFBasic)

```
"Properties": {  
    "SubnetId": {  
        "Ref": "PublicSubnet2"  
    },  
    "RouteTableId": {  
        "Ref": "PublicRouteTable"  
    }  
},  
},
```

8) Resources – RouteTable & Route & Association (Private)

- Private Subnet 1,2와 NAT Gateway

```
"PrivateRouteTable1": {  
    "Type": "AWS::EC2::RouteTable",  
    "DependsOn": "VPC",  
    "Properties": {  
        "VpcId": {  
            "Ref": "VPC"  
        },  
        "Tags": [  
            {  
                "Key": "Name",  
                "Value": "Private1"  
            }  
        ]  
    }  
},  
"PrivateRouteTable2": {  
    "Type": "AWS::EC2::RouteTable",  
    "DependsOn": "VPC",  
    "Properties": {  
        "VpcId": {  
            "Ref": "VPC"  
        },  
    }  
},
```

Project – 2. CloudFormation (TFBasic)

```
"Tags": [
    {
        "Key": "Name",
        "Value": "Private2"
    }
],
},
"PrivateRoute1": {
    "Type": "AWS::EC2::Route",
    "DependsOn": [
        "PrivateRouteTable1",
        "AttachGateway"
    ],
    "Properties": {
        "RouteTableId": {
            "Ref": "PrivateRouteTable1"
        },
        "DestinationCidrBlock": "0.0.0.0/0",
        "NatGatewayId": {
            "Ref": "NATGateway"
        }
    }
},
"PrivateRoute2": {
    "Type": "AWS::EC2::Route",
    "DependsOn": [
        "PrivateRouteTable2",
        "AttachGateway"
    ],
    "Properties": {
        "RouteTableId": {
            "Ref": "PrivateRouteTable2"
        },
        "DestinationCidrBlock": "0.0.0.0/0",
        "NatGatewayId": {
            "Ref": "NATGateway2"
        }
    }
}
```

Project – 2. CloudFormation (TFBasic)

```
        },
    },
    "PrivateSubnet1RouteTableAssociation": {
        "Type": "AWS::EC2::SubnetRouteTableAssociation",
        "DependsOn": "PrivateRouteTable1",
        "Properties": {
            "SubnetId": {
                "Ref": "PrivateSubnet1"
            },
            "RouteTableId": {
                "Ref": "PrivateRouteTable1"
            }
        }
    },
    "PrivateSubnet2RouteTableAssociation": {
        "Type": "AWS::EC2::SubnetRouteTableAssociation",
        "DependsOn": "PrivateRouteTable2",
        "Properties": {
            "SubnetId": {
                "Ref": "PrivateSubnet2"
            },
            "RouteTableId": {
                "Ref": "PrivateRouteTable2"
            }
        }
    },
}
```

9) Resources – Security Group

"CommandHostSecurityGroup": {	=> Security Group 이름
"Type": "AWS::EC2::SecurityGroup",	=> Security Group 생성
"DependsOn": "AttachGateway",	
"Properties": {	
"GroupDescription": "Security Group for Command Host",	
"GroupName": "CommandHostSecurityGroup",	

Project – 2. CloudFormation (TFBasic)

```
"VpcId": {  
    "Ref": "VPC"                      => VPC 지정  
},  
"Tags": [  
    {  
        "Key": "Name",  
        "Value": "CommandHostSecurityGroup"  
    }  
],  
"SecurityGroupIngress": [  
    {  
        "IpProtocol": "tcp",           => 허용할 Port 지정  
        "FromPort": 22,  
        "ToPort": 22,  
        "CidrIp": "0.0.0.0/0"  
    }  
]  
}  
,  
"HTTPAccess": {  
    "Type": "AWS::EC2::SecurityGroup",  
    "Properties": {  
        "GroupDescription": "Allow HTTP access to client.",  
        "GroupName": "HTTPAccess",  
        "VpcId": {  
            "Ref": "VPC"  
        },  
        "Tags": [  
            {  
                "Key": "Name",  
                "Value": "HTTPAccess"  
            }  
        ],  
        "SecurityGroupIngress": [  
            {  
                "IpProtocol": "tcp",  
                "FromPort": 80,  
                "ToPort": 80,  
            }  
        ]  
    }  
}
```

Project – 2. CloudFormation (TFBasic)

```
        "Cidrlp": "0.0.0.0/0"
    },
    {
        "IpProtocol": "tcp",
        "FromPort": 443,
        "ToPort": 443,
        "Cidrlp": "0.0.0.0/0"
    },
    {
        "IpProtocol": "tcp",
        "FromPort": 22,
        "ToPort": 22,
        "Cidrlp": "0.0.0.0/0"
    }
]
}
},
}
```

10) Resources – Instances (BastionHost 1,2)

```
"BastionHost": {
    "Type": "AWS::EC2::Instance",
    "DependsOn": [
        "PublicSubnet1",
        "CommandHostSecurityGroup",
        "AttachGateway"
    ],
    "Properties": {
        "KeyName": {
            "Ref": "KeyName"
        },
        "ImageId": {
            "Ref": "AmazonLinuxAMIID"
        },
        "InstanceType": "t2.micro",
    }
}, => Instance 이름
=> Instance 생성
=> Parameter에서 지정한 Key
=> Parameter에서 지정한 AMI
=> Instance Type
```

Project – 2. CloudFormation (TFBasic)

```
"NetworkInterfaces": [
    {
        "DeviceIndex": "0",
        "AssociatePublicIpAddress": true,
        "SubnetId": {
            "Ref": "PublicSubnet1"          => 생성할 위치 ( Subnet )
        },
        "GroupSet": [
            {
                "Ref": "CommandHostSecurityGroup"
            },
            {
                "Ref": "HTTPAccess"           => 적용할 Security Group
            }
        ]
    },
    "UserData": {                               => UserData 등록
        "Fn::Base64": { "Fn::Join": [ "", [
            "#!/bin/bash\n",
            "sudo yum -y update\n",
            "sudo amazon-linux-extras install epel -y\n",
            "sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-
release-latest-7.noarch.rpm\n",
            "sudo systemctl reboot\n",
            "sudo yum install -y httpd\n",
            "sudo systemctl start httpd\n",
            "sudo systemctl enable httpd\n",
            "sudo yum install ansible -y\n",
            "sudo ansible-galaxy collection install ansible.posix\n",
            "sudo yum -y install putty\n",
            "sudo yum -y install vim bash-completion\n"
        ] ]
    }
},
"Tags": [
    {
        "Key": "Name",

```

Project – 2. CloudFormation (TFBasic)

```
        "Value": "Bastion Host"
    }
]
}
},
"BastionHost2": {
    "Type": "AWS::EC2::Instance",
    "DependsOn": [
        "PublicSubnet2",
        "CommandHostSecurityGroup",
        "AttachGateway"
    ],
    "Properties": {
        "KeyName": {
            "Ref": "KeyName"
        },
        "ImageId": {
            "Ref": "AmazonLinuxAMIID"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "DeviceIndex": "0",
                "AssociatePublicIpAddress": true,
                "SubnetId": {
                    "Ref": "PublicSubnet2"
                },
                "GroupSet": [
                    {
                        "Ref": "CommandHostSecurityGroup"
                    },
                    {
                        "Ref": "HTTPAccess"
                    }
                ]
            }
        ],
        "UserData": {

```

Project – 2. CloudFormation (TFBasic)

```
"Fn::Base64": { "Fn::Join": [ "", [
    "#!/bin/bash\\n",
    "sudo yum -y update\\n",
    "sudo amazon-linux-extras install epel -y\\n",
    "sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-
release-latest-7.noarch.rpm\\n",
    "sudo systemctl reboot\\n",
    "sudo yum install -y httpd\\n",
    "sudo systemctl start httpd\\n",
    "sudo systemctl enable httpd\\n",
    "sudo yum install ansible -y\\n",
    "sudo ansible-galaxy collection install ansible.posix\\n",
    "sudo yum -y install putty\\n",
    "sudo yum -y install vim bash-completion\\n"
]]
},
},
"Tags": [
{
  "Key": "Name",
  "Value": "Bastion Host2"
}
]
},
},
```

11) Resources – Instances (WebServer 1,2)

```
"WebServer": {
  "Type": "AWS::EC2::Instance",
  "DependsOn": [
    "PrivateSubnet1",
    "CommandHostSecurityGroup",
    "HTTPAccess",
    "AttachGateway"
  ]
}
```

Project – 2. CloudFormation (TFBasic)

```
],
"Properties": {
    "KeyName": {
        "Ref": "KeyName"
    },
    "ImageId": {
        "Ref": "AmazonLinuxAMIID"
    },
    "InstanceType": "t2.micro",
    "NetworkInterfaces": [
        {
            "DeviceIndex": "0",
            "AssociatePublicIpAddress": true,
            "SubnetId": {
                "Ref": "PrivateSubnet1"
            },
            "GroupSet": [
                {
                    "Ref": "HTTPAccess"
                },
                {
                    "Ref": "CommandHostSecurityGroup"
                }
            ]
        }
    ],
    "UserData": {
        "Fn::Base64": {
            "Fn::Join": [
                "#!/bin/bash\n",
                "sudo yum -y update\n",
                "sudo amazon-linux-extras install epel -y\n",
                "sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm\n",
                "sudo systemctl reboot\n",
                "sudo yum install -y httpd\n",
                "sudo systemctl start httpd\n",
                "sudo systemctl enable httpd\n",
                "sudo rpm -ivh http://repo.zabbix.com/zabbix/5.0/rhel/7/x86\_64
            ]
        }
    }
}
```

Project – 2. CloudFormation (TFBasic)

```
/zabbix-agent-5.0.3-1.el7.x86_64.rpm\\n",
    "sudo yum localinstall http://repo.zabbix.com/zabbix/5.0/rhel/7/x86\_64/zabbix-agent-5.0.3-1.el7.x86\_64.rpm\\n"]
}

},
"Tags": [
{
    "Key": "Name",
    "Value": "Web Server"
}
]
},
"WebServer2": {
    "Type": "AWS::EC2::Instance",
    "DependsOn": [
        "PrivateSubnet2",
        "CommandHostSecurityGroup",
        "HTTPAccess",
        "AttachGateway"
    ],
    "Properties": {
        "KeyName": {
            "Ref": "KeyName"
        },
        "ImageId": {
            "Ref": "AmazonLinuxAMIID"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
{
            "DeviceIndex": "0",
            "AssociatePublicIpAddress": true,
            "SubnetId": {
                "Ref": "PrivateSubnet2"
            },
            "GroupSet": [
{

```

Project – 2. CloudFormation (TFBasic)

```
        "Ref": "HTTPAccess"
    },
    {
        "Ref": "CommandHostSecurityGroup"
    }
]
},
"UserData": {
    "Fn::Base64": { "Fn::Join": [ "", [
        "#!/bin/bash\\n",
        "sudo yum -y update\\n",
        "sudo amazon-linux-extras install epel -y\\n",
        "sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-
release-latest-7.noarch.rpm\\n",
        "sudo systemctl reboot\\n",
        "sudo yum install -y httpd\\n",
        "sudo systemctl start httpd\\n",
        "sudo systemctl enable httpd\\n",
        "sudo rpm -ivh
http://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-agent-5.0.3-
1.el7.x86_64.rpm\\n",
        "sudo yum localinstall
http://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-agent-5.0.3-
1.el7.x86_64.rpm\\n"]
    ]
},
    "Tags": [
        {
            "Key": "Name",
            "Value": "Web Server2"
        }
    ]
},
},
```

12) Resources – RDS

```
"DBEC2SecurityGroup": {  
    "Type": "AWS::EC2::SecurityGroup",  
    "Condition": "Is-EC2-VPC",  
    "Properties": {  
        "GroupDescription": "Open database for access",  
        "SecurityGroupIngress": [{  
            "IpProtocol": "tcp",  
            "FromPort": "3306",  
            "ToPort": "3306",  
            "SourceSecurityGroupName": { "Ref": "EC2SecurityGroup" }  
        }]  
    }  
},  
"DBSubnetGroup": {  
    "Type": "AWS::RDS::DBSubnetGroup",  
    "Properties": {  
        "DBSubnetGroupDescription": "SubnetGroup for MySQL RDS",  
        "DBSubnetGroupName": "DBSubnetGroup",  
        "SubnetIds": [  
            {"Ref": "PrivateSubnet3"},  
            {"Ref": "PrivateSubnet4"}  
        ]  
    }  
},  
"DBSecurityGroup": {  
    "Type": "AWS::RDS::DBSecurityGroup",  
    "Condition": "Is-EC2-Classic",  
    "Properties": {  
        "EC2VpcId": { "Ref": "VPC" },  
        "DBSecurityGroupIngress": {  
            "EC2SecurityGroupName": { "Ref": "EC2SecurityGroup" }  
        },  
        "GroupDescription": "database access"  
    }  
},
```

Project – 2. CloudFormation (TFBasic)

```
"MasterRDS": {                                     => MasterRDS로 사용할 DBInstance 이름
    "Type": "AWS::RDS::DBInstance",                => DB Instance 생성
    "Properties": {
        "DBName": { "Ref": "DBName" },             => Parameter에서 지정한 DB Name
        "AllocatedStorage": { "Ref": "DBAllocatedStorage" },   => Parameter
        "DBInstanceClass": { "Ref": "DBInstanceClass" },   => Parameter
        "Engine": "MySQL",                         => DB 엔진 지정
        "MasterUsername": { "Ref": "DBUser" },          => Parameter
        "MasterUserPassword": { "Ref": "DBPassword" },     => Parameter
        "AvailabilityZone": {
            "Fn::Select": [
                "0",                                     => 가용영역 ( a )
                {
                    "Fn::GetAZs": {
                        "Ref": "AWS::Region"
                    }
                }
            ]
        },
        "Tags": [{ "Key": "Name", "Value": "Master RDS" }],
        "VPCSecurityGroups": { "Fn::If": [ { "Is-EC2-VPC": [ { "Fn::GetAtt": [ "DBEC2SecurityGroup", "GroupId" ] } ], { "Ref": "AWS::NoValue" } ] },
        "DBSecurityGroups": { "Fn::If": [ { "Is-EC2-Classic": [ { "Ref": "DBSecurityGroup" } ], { "Ref": "AWS::NoValue" } ] }
        },
        "DeletionPolicy": "Snapshot"
    },
    "ReplicaRDS": {
        "Type": "AWS::RDS::DBInstance",
        "Properties": {
            "SourceDBInstanceIdentifier": { "Ref": "MasterRDS" },           => MasterRDS의 데이터 공유
            "DBInstanceClass": { "Ref": "DBInstanceClass" },                  => Parameter
            "AvailabilityZone": {
                "Fn::Select": [
                    "2",                                     => 가용영역 ( c )
                    {

```

Project – 2. CloudFormation (TFBasic)

```
        "Fn::GetAZs": {
            "Ref": "AWS::Region"
        }
    ],
},
"Tags": [{ "Key" : "Name", "Value" : "Replica RDS" }]
}
},
},
},
```

13) Outputs

```
"Outputs": {
    "AMIID": {
        "Value": {
            "Ref": "AmazonLinuxAMIID"
        }
    },
    "COMMANDHOSTIP": {
        "Value": {
            "Fn::Sub": "${BastionHost.PublicIp}"
        }
    },
    "KEYNAME": {
        "Value": {
            "Ref": "KeyName"
        }
    },
    "HTTPACCESS": {
        "Value": {
            "Ref": "HTTPAccess"
        }
    },
    "SUBNETID": {
        "Value": {
```

Project – 2. CloudFormation (TFBasic)

```
        "Ref": "PublicSubnet1"
    }
},
"EC2Platform" : {
    "Description" : "Platform in which this stack is deployed",
    "Value" : { "Fn::If" : [ "Is-EC2-VPC", "EC2-VPC", "EC2-Classic" ] }
},

"MasterJDBCConnectionString": {
    "Description" : "JDBC connection string for the master database",
    "Value" : { "Fn::Join": [ "", [ "jdbc:mysql://",
        { "Fn::GetAtt": [ "MasterRDS", "Endpoint.Address" ] },
        ":" ,
        { "Fn::GetAtt": [ "MasterRDS", "Endpoint.Port" ] },
        "/",
        { "Ref": "DBName" }]]}
},
"ReplicaJDBCConnectionString": {
    "Description" : "JDBC connection string for the replica database",
    "Value" : { "Fn::Join": [ "", [ "jdbc:mysql://",
        { "Fn::GetAtt": [ "ReplicaRDS", "Endpoint.Address" ] },
        ":" ,
        { "Fn::GetAtt": [ "ReplicaRDS", "Endpoint.Port" ] },
        "/",
        { "Ref": "DBName" }]]}
}
}
```

14) CloudFormation Upload

- 등록 방법은 1. CloudFormation (TFUser) 참고

- Stack 이름 입력

Project – 2. CloudFormation (TFBasic)

Specify stack details

Stack name

Stack name
FTBasic

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

- Parameter 값 입력
(일부는 미입력시 기본값으로 지정)

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

AmazonLinuxAMID AMI
/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2

DBAllocatedStorage
The size of the database (Gb)
5

DBInstanceClass
The database instance type
db.t2.micro

DBName
The database name
RDSDatabase

DBPassword
The database admin account password

DBUser
The database admin account username
....

EC2SecurityGroup
The EC2 security group that contains instances that need access to the database
default

KeyName
Name of an existing EC2 KeyPair to enable SSH access to the instance
Key Pair 등록
20211026_Keypair

MultiAZ
Multi-AZ master database
false

Project – 2. CloudFormation (TFBasic)

PrivateSubnet1Param
Private Subnet 1
10.5.50.0/24

CIDR 지정
(미입력시 기본값 적용)

PrivateSubnet2Param
Private Subnet 2
10.5.100.0/24

PrivateSubnet3Param
Private Subnet 3
10.5.60.0/24

PrivateSubnet4Param
Private Subnet 4
10.5.110.0/24

PublicSubnet1Param
Public Subnet 1
10.5.10.0/24

PublicSubnet2Param
Public Subnet 2
10.5.20.0/24

VPCCIDR
CIDR Block for VPC
10.5.0.0/16

Cancel Previous **Next**

- 설정사항 체크 후에 Create stack

► Quick-create link

The template has changed
CloudFormation has detected changes between the template uploaded and the one being used for this operation. Verify that the changes are intentional.

I acknowledge that the template used for this operation may contain changes that are different from the template uploaded through the console.

Cancel Previous **Create stack**

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

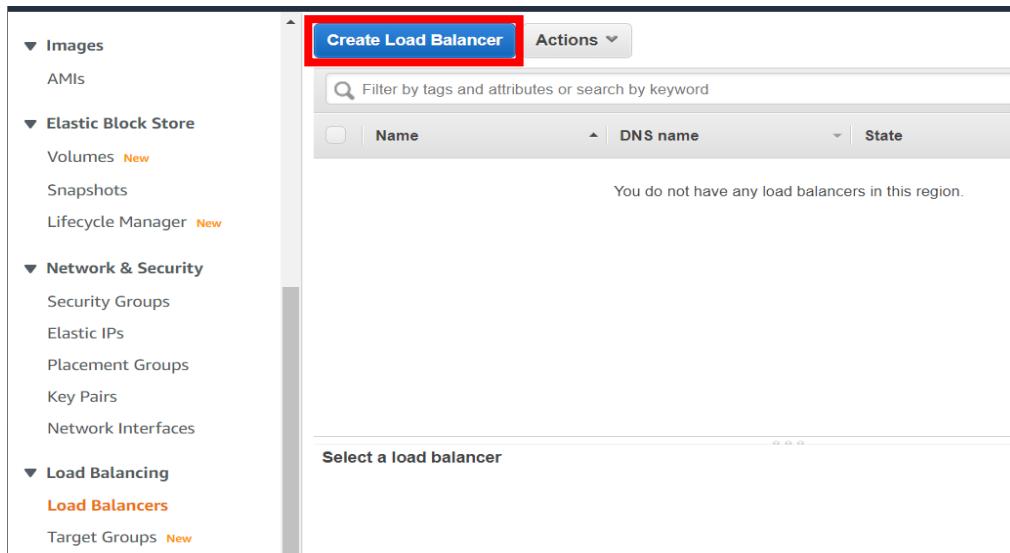
- 생성 확인

FTbasic					
Stack info	Events	Resources	Outputs	Parameters	Template
Events (37+)					
	<input type="text"/> com				
Timestamp	Logical ID	Status	Status reason		
2021-11-01 15:16:22 UTC+0900	FTbasic	CREATE_COMPLETE	-		
2021-11-01 15:16:17 UTC+0900	ReplicaRDS	CREATE_COMPLETE	-		
2021-11-01 15:03:25 UTC+0900	MasterRDS	CREATE_COMPLETE	-		

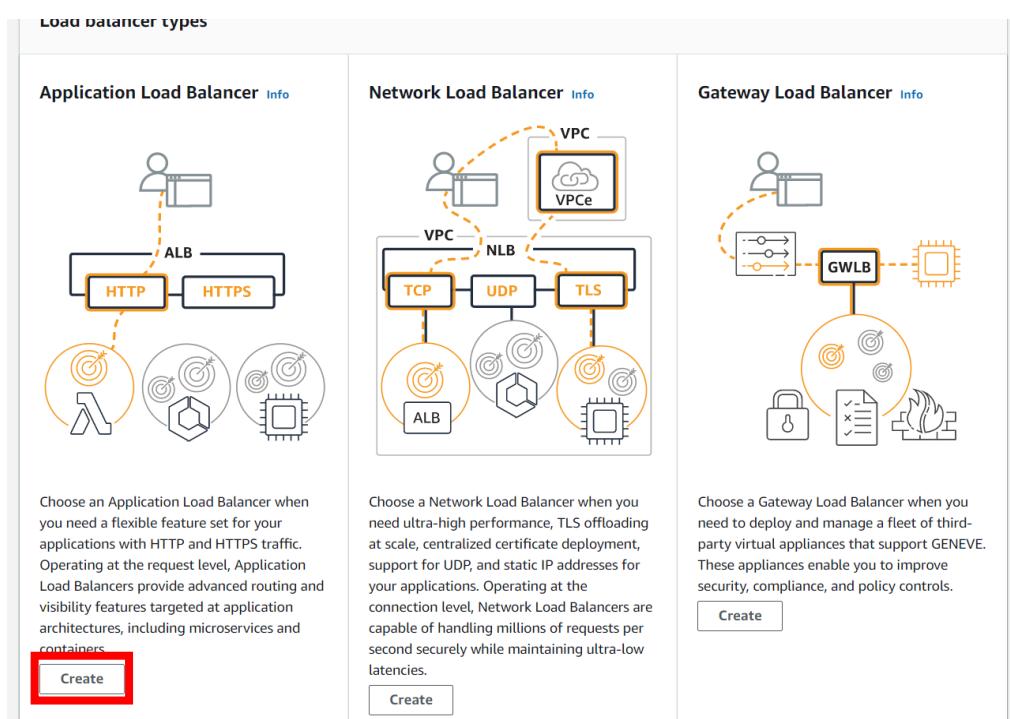
Project – 3. Load Balancing

3. Load Balancing

- EC2 > Load Balancers > Create Load Balancer



- ALB (Application Load Balancer) Create



Project – 3. Load Balancing

– Load Balancer Basic Configuration

- Name : WEBServer
- Scheme : Internet-facing
- IP address type : IPv4

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

► **How Application Load Balancers work**

Basic configuration

Load balancer name
The load balancer name must be unique within your AWS account and cannot be changed after the load balancer is created.
 WEBServer

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info
Scheme cannot be changed after the load balancer is created.
 Internet-facing
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#) Info
 Internal
An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type Info
Select the type of IP addresses that your subnets use.
 IPv4
Recommended for internal load balancers.
 Dualstack
Includes IPv4 and IPv6 addresses.

– VPC : FT VPC

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC Info
Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be confirmed until you select a target group. [View target groups](#) Info

FT VPC
vpc-064ed13ed70e314f6
IPv4: 10.5.0.0/16

Project – 3. Load Balancing

- Subnet : Private Subnet1 & Private Subnet2

The screenshot shows the 'Mappings' section of a load balancer configuration. It lists two Availability Zones (ap-northeast-2a and ap-northeast-2c) each associated with a private subnet. Both subnets are highlighted with a red box.

Mappings Info
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Available balancer or the VPC are not available for selection. Subnets cannot be removed after the load balancer is created, but additional subnets can be added.

ap-northeast-2a

Subnet: subnet-02fce225fef014d83 (Private Subnet 1)

IPv4 settings
Assigned by AWS

ap-northeast-2c

Subnet: subnet-08f00f2c9290ff56e (Private Subnet 2)

IPv4 settings
Assigned by AWS

- Security Group : HTTPAccess (기존의 Default는 삭제)

The screenshot shows the 'Security groups' section of a security group configuration. A single security group, 'HTTPAccess sg-0e705d4d2f67fbfb3', is selected and highlighted with a red box.

Security groups Info
A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups
Select security groups Create new security group []

HTTPAccess sg-0e705d4d2f67fbfb3 X
VPC: vpc-064ed13ed70e314f6

Project – 3. Load Balancing

- Target 그룹 생성 (기존의 Target Group이 있을 경우에는 바로 선택)

› Create target group

› Basic Configuration

› Target type : Instance

› Target Name : WebServer

› VPC : FT VPC

Listeners and routing Info

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification. You can specify multiple rules and multiple certificates per listener after the load balancer is created.

▼ Listener HTTP:80 Remove

Protocol	Port	Default action	Info
HTTP	: 80	Forward to	WebServer 1-65535

[Create target group](#) []

[Add listener](#)

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Name [] WebServer
phanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol Port

HTTP : 80

VPC [] FT VPC
vpc-064ed13ad70e314f6
IPv4: 10.5.0.0/16

Protocol version

HTTP1 Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

HTTP2 Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

gRPC Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Project – 3. Load Balancing

› Health Checks

› Advanced health check settings

› Health threshold : 5

› Interval : 30

› Success codes : 200

▶ 30초마다 요청을 보내고 응답이 200번으로 5번 연속으로 오면 정상

▶ 200번 외의 코드가 오거나 5초 동안 응답이 없는 상태가 2번 연속이면 비정상

Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol
HTTP

Health check path
Use the default path of "/" to ping the root, or specify a custom path if preferred.
/

Up to 1024 characters allowed.

▼ Advanced health check settings Restore defaults

Port
The port the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer, but you can specify a different port.

Traffic port
 Override

Healthy threshold
The number of consecutive health checks successes required before considering an unhealthy target healthy.
5
2-10

Unhealthy threshold
The number of consecutive health check failures required before considering a target unhealthy.
2
2-10

Timeout
The amount of time, in seconds, during which no response means a failed health check.
5 seconds
2-120

Interval
The approximate amount of time between health checks of an individual target.
30 seconds
5-300

Success codes
The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").
200

► Tags - optional
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel Next

Project – 3. Load Balancing

- Target 등록

› Web server 1,2 체크 후에 Include as pending below 클릭해서 등록

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/4)

Instance ID	Name	State	Security groups	Zone	Subnet ID
<input checked="" type="checkbox"/> i-0bf454524e093032c	Web Server	running	CommandHostSecurityGroup, HTTPAccess	ap-northeast-2a	subnet-02fce225fef014d83
<input type="checkbox"/> i-019cbc4bb1a239c15	Command Host	running	CommandHostSecurityGroup	ap-northeast-2a	subnet-0874892a74df41275
<input type="checkbox"/> i-0831946c0cac76cec	Command Host2	running	CommandHostSecurityGroup	ap-northeast-2c	subnet-00567218c87e18269
<input checked="" type="checkbox"/> i-0d90d7bbcc3928858	Web Server2	running	CommandHostSecurityGroup, HTTPAccess	ap-northeast-2c	subnet-08f00f2c9290ff56e

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances:
80
1-65535 (separate multiple ports with commas)

Include as pending below

2 selections are now pending below. Include more or register targets when ready.

Review targets

Targets (2)

Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	Subnet ID
X	Pending	i-0d90d7bbcc3928858	Web Server2	80	running	CommandHostSecurityGroup, HTTPAccess	ap-northeast-2c	subnet-08f00f2c9290ff56e
X	Pending	i-0bf454524e093032c	Web Server	80	running	CommandHostSecurityGroup, HTTPAccess	ap-northeast-2a	subnet-02fce225fef014d83

2 pending

Cancel Previous Create target group

› Target Group 생성후에 다시 Load Balacing 생성 페이지로 돌아와서 등록

(만약 보이지 않는다면 Target Group 새로고침)

Listeners and routing Info

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification. You can specify multiple rules and multiple certificates per listener after the load balancer is created.

▼ Listener HTTP:80

Protocol	Port	Default action	Info
HTTP	: 80	Forward to	WebServer Target type: Instance, IPv4

C

Add listener

Project – 4. Auto Scaling

- 설정 확인하고 Create

The screenshot shows the 'Summary' step of creating a load balancer. It includes sections for 'Basic configuration', 'Security groups', 'Network mapping', and 'Listeners and routing'. A note indicates default attributes will be applied to the load balancer after creation. At the bottom right are 'Cancel' and 'Create load balancer' buttons.

Basic configuration Edit		Security groups Edit	Network mapping Edit	Listeners and routing Edit
WEBServer	• Internet-facing • IPv4	• HTTPAccess sg-0e705d4d2f67fbfb3	VPC vpc-064ed13ed70e314f6 FT VPC • ap-northeast-2a subnet-02fce25fef014db3 Private Subnet 1 • ap-northeast-2c subnet-08f00f2c9290ff56e Private Subnet 2	• HTTP:80 defaults to WebServer

Tags Edit
None

Attributes

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Cancel **Create load balancer**

4. Auto Scaling

1) AMI 생성

- 시작구성 생성에 사용할 AMI 생성
 - EC2 > Instance > Web Server (이미지 생성을 원하는 인스턴스) 선택
 - > Action > Image and Templates > Create image

The screenshot shows the 'Instances' page with two instances listed: 'Web Server' and 'Bastion Host'. The 'Actions' menu for the 'Web Server' instance is open, highlighting the 'Create image' and 'Image and templates' options. These options are also highlighted with red boxes in the image.

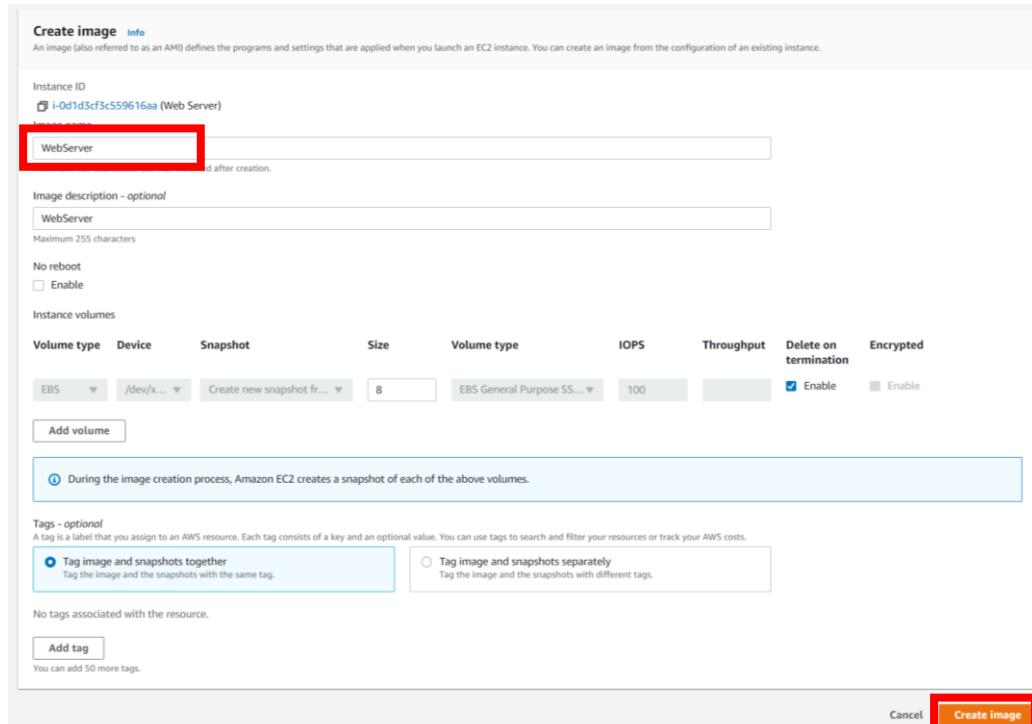
Name	Instance ID	Instance state	Instance type	Status check	Alarm state
Web Server	i-0d1d3cf3c559616aa	Running	t2.micro	2/2 checks passed	No alarm
Bastion Host	i-021f9c66833fe39ff	Running	t2.micro	2/2 checks passed	No alarm
Web Server2	i-0581a04c3752fa0fc	Running	t2.micro	2/2 checks passed	No alarm
Bastion Host2	i-01892ee6e9ecd3cc4	Running	t2.micro	2/2 checks passed	No alarm

Actions ▾ Launch instances

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Create image**
- Image and templates**
- Launch more like this

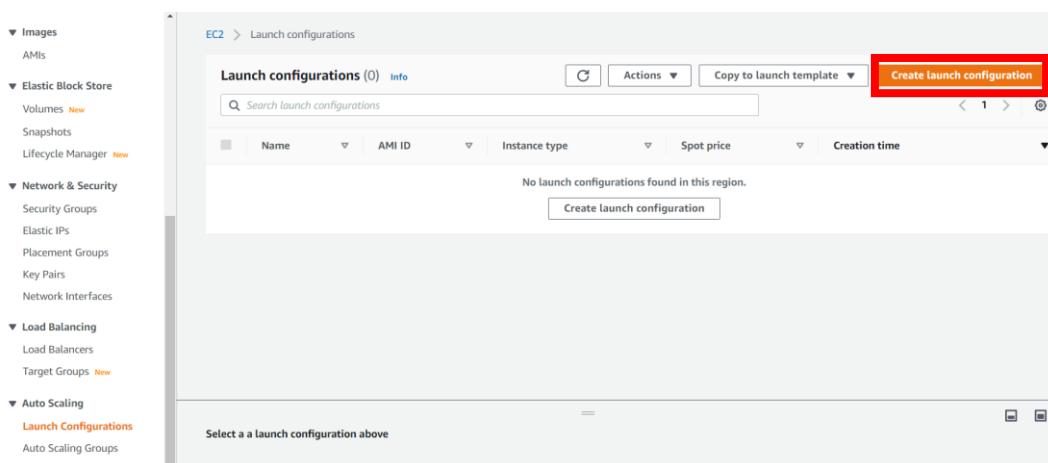
Project – 4. Auto Scaling

- 이름 지정 후 Create



2) Configurations (시작구성) 생성

- EC2 > Launch Configuration > Create launch configuration



Project – 4. Auto Scaling

- Configuration 정보 입력

› Name : WEB-config

› AMI : Web-AMI

› Instance type

Create launch configuration [Info](#)

Launch configuration name

Name WEB-config

Amazon machine image (AMI) [Info](#)

AMI Web-AMI

Instance type [Info](#)

Instance type Choose instance type

- Monitoring : Enable 체크

Additional configuration - optional

Purchasing option [Info](#)
 Request Spot Instances

IAM instance profile [Info](#)

Monitoring [Info](#)
 Enable EC2 instance detailed monitoring within CloudWatch

EBS-optimized instance
 Launch as EBS-optimized instance

► Advanced details

Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations cannot be edited.

Project – 4. Auto Scaling

- Security Group : HTTPAccess

The screenshot shows the AWS Security Groups page. At the top, there are two options: 'Create a new security group' (radio button) and 'Select an existing security group' (radio button, which is selected and highlighted with a red box). Below this is a search bar labeled 'Search security groups'. A table lists several security groups:

Security group ID	Name	VPC ID	Description
sg-02e02596ceaae7fad	FTbasic-DBEC2SecurityGroup-9SP5906L4KUY	vpc-0333feeebb4b014fe	Open database for access
sg-02e9d0846120f4523	HTTPAccess	vpc-02f89db8a02dd7d48	Allow HTTP access to client.
sg-05434cd4ccc728b87	default	vpc-0333feeebb4b014fe	default VPC security group
sg-0b318df2af5e99e16	CommandHostSecurityGroup	vpc-02f89db8a02dd7d48	Security Group for Command Host
sg-0b611b2d607f2370b	default	vpc-02f89db8a02dd7d48	default VPC security group

- Key Pair 선택 후 Create

The screenshot shows the AWS Key pair (login) configuration page. It includes fields for 'Key pair options' (choose an existing key pair), 'Existing key pair' (selected as '20211026_Keypair'), and a checkbox for acknowledging access to the private key file. At the bottom right are 'Cancel' and 'Create launch configuration' buttons, with 'Create launch configuration' highlighted with a red box.

3) Auto Scaling 그룹 / 정책 설정

- 2)에서 생성한 시작구성 > Action > Create Auto Scaling group

The screenshot shows the AWS Launch configurations page. It displays a table with one entry ('WEB-config') and includes columns for Name, AMI ID, Instance type, and Creation time. At the top right, there are buttons for 'Actions', 'Copy to launch template', and 'Create launch configuration'. A context menu is open over the 'Actions' button, with the 'Create Auto Scaling group' option highlighted with a red box.

Project – 4. Auto Scaling

- Auto Scaling Group 정보입력

› Name : Web-Auto

Choose launch template or configuration Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name
Auto Scaling group name Enter a name to identify the group. WEB-Auto

Must be unique to this account in the current Region and no more than 255 characters.

- Instance Option 설정

› VPC : FT VPC

› Subnet : Private Subnet 1 , Private Subnet 2

Choose instance launch options Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Network <small>Info</small>
For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.
VPC Choose the VPC that defines the virtual network for your Auto Scaling group. vpc-02f89db8a02dd7d48 (FT VPC)
Create a VPC
Availability Zones and subnets Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.
Select Availability Zones and subnets
ap-northeast-2a subnet-070d14076f34d7b1e (Private Subnet 1) 10.5.50.0/24
ap-northeast-2c subnet-0b6bac3a86893fc8 (Private Subnet 2) 10.5.100.0/24
Create a subnet

Cancel Previous Skip to review **Next**

Project – 4. Auto Scaling

- Configure advanced options

- › Attach to an existing load balancer
 - › Choose from your load balancer target groups
 - › Target Group : WebServer
- › Monitoring : Enable

Configure advanced options Info

Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.

Load balancing - optional Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer
Choose from your existing load balancers.

Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

Existing load balancer target groups
Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

Web-TargetGroup | HTTP
Application Load Balancer: Web-ALB

Health checks - optional

Health check type Info
EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

EC2 ELB

Health check grace period
The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are put into service.

300 seconds

Additional settings - optional

Monitoring Info
 Enable group metrics collection within CloudWatch

Project – 4. Auto Scaling

- Group Size

- › Desired capacity : 원하는 크기
- › Minimum capacity : 최소크기 , 사용량이 남아도 최소크기 만큼의 인스턴스 유지
- › Maximum capacity : 최대크기 , 사용량이 부족할 경우 추가될수 있는 최대 인스턴스

Configure group size and scaling policies Info

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - optional Info

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity
2

Minimum capacity
2

Maximum capacity
4

Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. Info

Target tracking scaling policy
Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

None

Scaling policy name
Target Tracking Policy

Metric type
Average CPU utilization

Target value
50

Instances need
300 seconds warm up before including in metric

Disable scale in to create only a scale-out policy

Instance scale-in protection - optional

Instance scale-in protection
If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

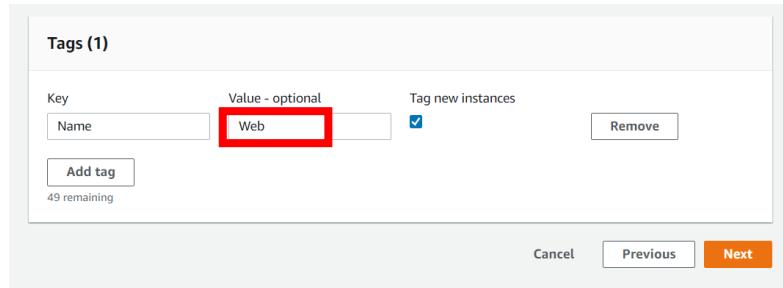
Enable instance scale-in protection

Buttons

Cancel Previous Skip to review Next

Project – 4. Auto Scaling

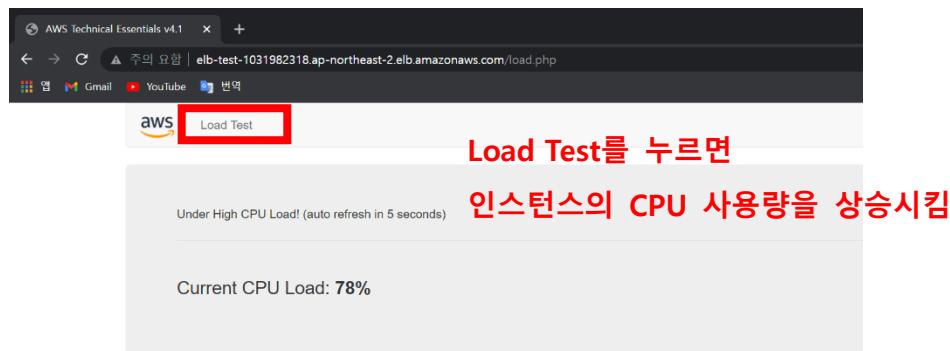
- Tag : Name – Web



- Review에서 설정한 내용확인 후 Create

4) Load Test

- EC2 > Load Balancer > Description > DNS name의 주소로 웹브라우저 열기



- CloudWatch > Alarms > In alarm 변경 확인



Project – 5. Video On Demand

- EC2 Instance에서 인스턴스 추가된 것 확인

인스턴스 (2/6) 정보										인스턴스 시작	
		C	연결	인스턴스 상태	작업						
인스턴스 필터링		<	1	>	②						
Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	피블릭 IPv4 DNS				
Bastion Host	i-0d2629748bc077d84	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	+ ap-northeast-2a	ec2-13-125-85-4				
Bastion Host2	i-0826cd1a346ba9e96	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	+ ap-northeast-2c	ec2-13-124-232-				
<input checked="" type="checkbox"/> Web	i-042cc74faf7a19cc1	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	+ ap-northeast-2a	-				
<input checked="" type="checkbox"/> Web	i-09f2a75f0df216bbb	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	+ ap-northeast-2c	-				
Web Server	i-0167f880fc799757d	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	+ ap-northeast-2a	ec2-13-124-201-				
Web Server2	i-0da9eade9d25b7886	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	+ ap-northeast-2c	ec2-3-37-36-33.e				

5. Video On Demand (CloudFormation)

{

"Description": "(SO0146) v1.1.0: Video on Demand on AWS Foundation Solution Implementation",

"Mappings": {

"Send": {

"AnonymousUsage": {

"Data": "Yes"

=> 익명 사용자 사용 가능

}

}

,

"Parameters": {

"emailAddress": {

"Type": "String",

"AllowedPattern": "^[A-Za-z0-9-]+(\.[A-Za-z0-9-]+)*@[A-Za-z0-9-]+\(\.[A-Za-z0-9-]+\)*(\.\{2,\})\$",

=> 이메일 규격 설정

Project – 5. Video On Demand

```
    "Description": "The admin email address to receive SNS notifications for job status."
}

},
"Resources": {
    "Logs6819BB44": {
        "Type": "AWS::S3::Bucket",
        "Properties": {
            "AccessControl": "LogDeliveryWrite",
            "BucketEncryption": {
                "ServerSideEncryptionConfiguration": [
                    {
                        "ServerSideEncryptionByDefault": {
                            "SSEAlgorithm": "AES256"
                        }
                    }
                ]
            },
            "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": true,
                "BlockPublicPolicy": true,
                "IgnorePublicAcls": true,
                "RestrictPublicBuckets": true
            }
        },
    }
},
```

Project – 5. Video On Demand

```
"UpdateReplacePolicy": "Retain",      => 스택 업데이트 작업 중 리소스의 기존 물리적  
                                         인스턴스가 교체될 때 보존하거나 백업가능  
"DeletionPolicy": "Retain",           => 스택이 삭제될 때 리소스를 보존 or 백업  
"Metadata": {  
    "cfn_nag": {  
        "rules_to_suppress": [  
            {  
                "id": "W35",  
                "reason": "Logs bucket does not require logging configuration"  
            },  
            {  
                "id": "W51",  
                "reason": "Logs bucket is private and does not require a bucket policy"  
            }  
        ]  
    }  
},  
"Source71E471F1": {  
    "Type": "AWS::S3::Bucket",  
    "Properties": {  
        "BucketEncryption": {  
            "ServerSideEncryptionConfiguration": [  
                {  
                    "awsKmsMasterKeyArn": "arn:aws:kms:ap-northeast-2:123456789012:alias/VideoOnDemand",  
                    "serverSideEncryption": "aws:kms"  
                }  
            ]  
        }  
    }  
}
```

Project – 5. Video On Demand

```
        "ServerSideEncryptionByDefault":  
            "SSEAlgorithm": "AES256"  
        }  
    }  
]  
,  
"LoggingConfiguration": {  
    "DestinationBucketName": {  
        "Ref": "Logs6819BB44"  
    },  
    "LogFilePrefix": "source-bucket-logs/"  
},  
"PublicAccessBlockConfiguration": {  
    "BlockPublicAcls": true,  
    "BlockPublicPolicy": true,  
    "IgnorePublicAcls": true,  
    "RestrictPublicBuckets": true  
}  
,  
"UpdateReplacePolicy": "Retain",  
"DeletionPolicy": "Retain",  
"Metadata": {  
    "cfn_nag": {  
        "rules_to_suppress": [  

```

Project – 5. Video On Demand

```
        "id": "W51",
        "reason": "source bucket is private and does not require a bucket policy"
    }
]
}
},
"Destination920A3C57": {
    "Type": "AWS::S3::Bucket",
    "Properties": {
        "BucketEncryption": {
            "ServerSideEncryptionConfiguration": [      => 서버 측 암호화 구성
            {
                "ServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256"
                }
            }
        ]
    },
    "CorsConfiguration": {      => 타 출처자원공유를 할 수 있도록 설정하는 권한체제
        "CorsRules": [
            {
                "AllowedHeaders": [

```

Project – 5. Video On Demand

```
"*"  
    => 모든 헤더 허용  
],  
"AllowedMethods": [  
    "GET"  
        => GET 매서드 허용  
],  
"AllowedOrigins": [  
    "*"  
        => 모든 Origins 허용  
],  
"MaxAge": 3000  
        => 실행 전 요청결과를 캐시할 수 있는 시간  
}  
]  
},  
"LoggingConfiguration": {  
    "DestinationBucketName": {  
        "Ref": "Logs6819BB44"  
    },  
    "LogFilePrefix": "destination-bucket-logs/"  
},  
"PublicAccessBlockConfiguration": {  
    "BlockPublicAcls": true,  
    "BlockPublicPolicy": true,  
    "IgnorePublicAcls": true,  
    "RestrictPublicBuckets": true  
}
```

Project – 5. Video On Demand

```
        "UpdateReplacePolicy": "Retain",
        "DeletionPolicy": "Retain",
        "Metadata": {
            "aws:cdk:path": "VodFoundation/Destination/Resource"
        }
    },
    "DestinationPolicy7982387E": {
        "Type": "AWS::S3::BucketPolicy",
        "Properties": {
            "Bucket": {
                "Ref": "Destination920A3C57"
            },
            "PolicyDocument": {
                "Statement": [
                    {
                        "Action": "s3:GetObject",          => S3에서 객체를 가져온다.
                        "Effect": "Allow",
                        "Principal": {
                            "CanonicalUser": {
                                "Fn::GetAtt": [
                                    "CloudFrontCloudFrontDistributionOrigin1S3Origin17B88F1A",
                                    "S3CanonicalUserId"      => S3 규범 사용자 id
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Project – 5. Video On Demand

```
    },
    ],
    "Resource": {
        "Fn::Join": [
            "",
            [
                {
                    "Fn::GetAtt": [
                        "Destination920A3C57",
                        "Arn"
                    ]
                }
            ],
            [
                {
                    "Fn::Join": [
                        [
                            {
                                "Fn::GetAtt": [
                                    "Destination920A3C57",
                                    "Arn"
                                ]
                            }
                        ],
                        [
                            {
                                "Fn::Join": [
                                    [
                                        {
                                            "Fn::GetAtt": [
                                                "Destination920A3C57",
                                                "Arn"
                                            ]
                                        }
                                    ],
                                    [
                                        {
                                            "Fn::Join": [
                                                [
                                                    {
                                                        "Fn::GetAtt": [
                                                            "Destination920A3C57",
                                                            "Arn"
                                                        ]
                                                    }
                                                ],
                                                [
                                                    {
                                                        "Fn::Join": [
                                                            [
                                                                {
                                                                    "Fn::GetAtt": [
                                                                        "Destination920A3C57",
                                                                        "Arn"
                                                                    ]
                                                                }
                                                            ],
                                                            [
                                                                {
                                                                    "Fn::Join": [
                                                                        [
                                                                            {
                                                                                "Fn::GetAtt": [
                                                                                    "Destination920A3C57",
                                                                                    "Arn"
                                                                                ]
                                                                            }
                                                                        ],
                                                                        [
                                                                            {
                                                                                "Fn::Join": [
                                                                                    [
                                                                

```

Project – 5. Video On Demand

```
        "id": "F16",
        "reason": "Public website bucket policy requires a wildcard principal"
    }
]
}
},
"CloudFrontCloudfrontLoggingBucketE23C521E": {
    "Type": "AWS::S3::Bucket",
    "Properties": {
        "AccessControl": "LogDeliveryWrite",
        "BucketEncryption": {
            "ServerSideEncryptionConfiguration": [
                {
                    "ServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "AES256"
                    }
                }
            ]
        },
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicIp": true
        }
    }
}
```

Project – 5. Video On Demand

```
"IgnorePublicAcls": true,  
  
"RestrictPublicBuckets": true  
  
},  
  
"VersioningConfiguration": {  
    "Status": "Enabled"          => 버킷 버전관리 허용  
}  
  
},  
  
"UpdateReplacePolicy": "Retain",  
  
"DeletionPolicy": "Retain",  
  
"Metadata": {  
  
    "cfn_nag": {  
  
        "rules_to_suppress": [  
  
            {  
  
                "id": "W35",  
  
                "reason": "This S3 bucket is used as the access logging bucket for CloudFront  
Distribution"  
  
            }  
  
        ]  
  
    }  
  
},  
  
},  
  
"CloudFrontCloudfrontLoggingBucketPolicyD60AA01A": {  
  
    "Type": "AWS::S3::BucketPolicy",  
  
    "Properties": {  
  
        "Bucket": {
```

Project – 5. Video On Demand

```
"Ref": "CloudFrontCloudfrontLoggingBucketE23C521E"  
},  
"PolicyDocument": {  
    "Statement": [  
        {  
            "Action": "*",  
            "Condition": {  
                "Bool": {  
                    "aws:SecureTransport": "false"      => 객체에 대한 모든 작업을 거부  
                }  
            },  
            "Effect": "Deny",  
            "Principal": "*",  
            "Resource": {  
                "Fn::Join": [  
                    "",  
                    [  
                        {  
                            "Fn::GetAtt": [  
                                "CloudFrontCloudfrontLoggingBucketE23C521E",  
                                "Arn"  
                            ]  
                        },  
                        /*  
                ],  
                "Ref": "CloudFrontCloudfrontLoggingBucketE23C521E"  
            }  
        }  
    ]  
},  
"Version": "2012-10-17"
```

Project – 5. Video On Demand

```
        ],
        ],
    },
    "Sid": "HttpsOnly"    => https 만 허용, http 액세스 거부
},
],
"Version": "2012-10-17"
},
},
"Metadata": {
    "aws:cdk:path": "VodFoundation/CloudFront/CloudfrontLoggingBucket/Policy/Resource"
},
},
"CloudFrontCloudFrontDistributionOrigin1S3Origin17B88F1A": {
    "Type": "AWS::CloudFront::CloudFrontOriginAccessIdentity",    => 새 Origin 허용생성
    "Properties": {
        "CloudFrontOriginAccessIdentityConfig": {
            "Comment": "Identity for
VodFoundationCloudFrontCloudFrontDistributionOrigin1F191A578"
        }
    },
    "Metadata": {
        "aws:cdk:path": "VodFoundation/CloudFront/CloudFrontDistribution/Origin1/S3Origin/Resource"
    }
}
```

Project – 5. Video On Demand

```
}

},
"CloudFrontCloudFrontDistribution824F3346": {
    "Type": "AWS::CloudFront::Distribution",
    "Properties": {
        "DistributionConfig": { => 구성 정보
            "Comment": {
                "Fn::Join": [
                    "",
                    [
                        {
                            "Ref": "AWS::StackName"
                        },
                        " Video on Demand Foundation"
                    ]
                ]
            },
            "DefaultCacheBehavior": { => 기본 캐시 동작
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e58f6",
                "Compress": true, => 파일 자동 압축
                "TargetOriginId":
                "VodFoundationCloudFrontCloudFrontDistributionOrigin1F191A578",
                "ViewerProtocolPolicy": "redirect-to-https"
            }
        }
    }
}
=> 최종 사용자가 HTTP 요청을 제출하면 CloudFront는 HTTPS URL과 함께 HTTP 상태 코드 301을 반환하고 뷰어는 새 URL을 사용하여 요청을 다시 제출
```

Project – 5. Video On Demand

```
},  
    "DefaultRootObject": "index.html",           => 기본 루트 객체 지정  
    "Enabled": true,  
    "HttpVersion": "http2",  
    "IPV6Enabled": true,  
    "Logging": {  
        "Bucket": {  
            "Fn::GetAtt": [  
                "CloudFrontCloudfrontLoggingBucketE23C521E",  
                "RegionalDomainName"  
            ]  
        }  
    },  
    "Origins": [  
        {  
            "DomainName": {  
                "Fn::GetAtt": [  
                    "Destination920A3C57",  
                    "RegionalDomainName"  
                ]  
            },  
            "Id": "VodFoundationCloudFrontCloudFrontDistributionOrigin1F191A578",  
            "S3OriginConfig": {  
                "OriginAccessIdentity": {  

```

Project – 5. Video On Demand

Project – 5. Video On Demand

```
}

},

},
"MediaConvertRole031A64A9": {

  "Type": "AWS::IAM::Role",           => AWS 계정에 대한 새 Role을 생성

  "Properties": {

    "AssumeRolePolicyDocument": {

      "Statement": [

        {

          "Action": "sts:AssumeRole",           => 보통 액세스할 수 없는 리소스에

          "Effect": "Allow",                  사용할 수 있는 임시 보안 자격 증명

          "Principal": {

            "Service": "mediaconvert.amazonaws.com"

          }

        }

      ],
      "Version": "2012-10-17"
    }
  },
  "Metadata": {
    "aws:cdk:path": "VodFoundation/MediaConvertRole/Resource"
  }
},
```

Project – 5. Video On Demand

```
"MediaconvertPolicy9E3026EC": {  
    "Type": "AWS::IAM::Policy",  
    "Properties": {  
        "PolicyDocument": {  
            "Statement": [  
                {  
                    "Action": [  
                        "s3:GetObject",  
                        "s3:PutObject"  
                    ],  
                    "Effect": "Allow",  
                    "Resource": [  
                        {  
                            "Fn::Join": [  
                                "",  
                                [  
                                    {  
                                        "Fn::GetAtt": [  
                                            "Source71E471F1",  
                                            "Arn"  
                                        ]  
                                    },  
                                    {"  
                                ]  
                            },  
                            /*  
                        ]  
                    ]  
                }  
            ]  
        }  
    }  
}
```

=> 미디어 변환 정책

=> 객체 가져오기

=> 객체 추가하기

Project – 5. Video On Demand

```
        ],
    },
    {
        "Fn::Join": [
            "",
            [
                {
                    "Fn::GetAtt": [
                        "Destination920A3C57",
                        "Arn"
                    ]
                },
                /*
            ],
            ]
        }
    ],
    {
        "Action": "execute-api:Invoke",           => 클라이언트 요청 시 API를 호출
        "Effect": "Allow",
        "Resource": {
            "Fn::Join": [
                "",
                [
                    "arn:aws:execute-api::://"
                ]
            ]
        }
    }
},
```

Project – 5. Video On Demand

```
[  
    "arn:",  
    {  
        "Ref": "AWS::Partition"  
    },  
    ":execute-api:",  
    {  
        "Ref": "AWS::Region"  
    },  
    ":",  
    {  
        "Ref": "AWS::AccountId"  
    },  
    "*"  
]  
]  
}  
],  
"Version": "2012-10-17"  
},  
"PolicyName": "MediaconvertPolicy9E3026EC",  
"Roles": [  
{
```

Project – 5. Video On Demand

```
"Ref": "MediaConvertRole031A64A9"

}

],

"Metadata": {

    "aws:cdk:path": "VodFoundation/MediaconvertPolicy/Resource"
}

},



"CustomResourceServiceRoleE774390D": {           => 사용자 지정 리소스 Role

    "Type": "AWS::IAM::Role",

    "Properties": {

        "AssumeRolePolicyDocument": {

            "Statement": [

                {

                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {

                        "Service": "lambda.amazonaws.com"
                    }
                }
            ],
            "Version": "2012-10-17"
        },
        "ManagedPolicyArns": [           => 새 관리형 정책을 생성
            ...
        ]
    }
}
```

Project – 5. Video On Demand

Project – 5. Video On Demand

```
"Action": [  
    "s3:PutObject",  
    "s3:PutBucketNotification"      => 버킷에 지정된 이벤트알림을 활성화  
,  
    "Effect": "Allow",  
    "Resource": [  
        {  
            "Fn::GetAtt": [  
                "Source71E471F1",  
                "Arn"  
            ]  
        },  
        {  
            "Fn::Join": [  
                "",  
                [  
                    {  
                        "Fn::GetAtt": [  
                            "Source71E471F1",  
                            "Arn"  
                        ]  
                    },  
                    /*  
                ]  
            },  
            "/*"  
        ]  
    ]
```

Project – 5. Video On Demand

```
        ],
    }
],
},
{
    "Action": "mediaconvert:DescribeEndpoints",
        => 계정 API 엔드포인트를 가져오기위해 리전에 비어있는 요청을 전송
    "Effect": "Allow",
    "Resource": {
        "Fn::Join": [
            "",
            [
                "arn:aws:mediaconvert:",
                {
                    "Ref": "AWS::Region"
                },
                ".",
                {
                    "Ref": "AWS::AccountId"
                },
                ":*"
            ]
        ]
    }
}
```

Project – 5. Video On Demand

```
    },
],
"Version": "2012-10-17",
},
"PolicyName": "CustomResourceServiceRoleDefaultPolicy62213138",
"Roles": [
{
  "Ref": "CustomResourceServiceRoleE774390D"
}
],
},
"Metadata": {
  "aws:cdk:path": "VodFoundation/CustomResource/ServiceRole/DefaultPolicy/Resource"
},
"CustomResource8CDCD7A7": {
  "Type": "AWS::Lambda::Function",           => 람다 함수를 생성
  "Properties": {
    "Code": {
      "S3Bucket": {
        "Fn::Sub": "solutions-${AWS::Region}"
      },
      "S3Key": "video-on-demand-on-aws-  
foundation/v1.1.0/asset2bd7f95c3e5e8fd3883dadd70adcdb14c0f67bc3bbbe8be478beef5d"
    }
  }
}
```

Project – 5. Video On Demand

d78a2ae6.zip"

=> 배포 패키지의 Amazon S3 키

```
},  
"Role": {  
    "Fn::GetAtt": [  
        "CustomResourceServiceRoleE774390D",  
        "Arn"  
    ]  
},  
"Description": "CFN Custom resource to copy assets to S3 and get the MediaConvert  
endpoint",  
"Environment": {  
    "Variables": {  
        "SOLUTION_IDENTIFIER": "AwsSolution/SO0146/v1.1.0"  
    }  
},  
"Handler": "index.handler",  
"Runtime": "nodejs12.x",  
"Timeout": 30  
},  
"DependsOn": [          => 특정 리소스가 다른 리소스 다음에 생성되도록 지정  
    "CustomResourceServiceRoleDefaultPolicy62213138",  
    "CustomResourceServiceRoleE774390D"  
],  
"Metadata": {  
    "cfn_nag": {
```

Project – 5. Video On Demand

```
"rules_to_suppress": [
    {
        "id": "W58",
        "reason": "Invalid warning: function has access to cloudwatch"
    },
    {
        "id": "W89",
        "reason": "AWS Lambda does not require VPC for this solution."
    },
    {
        "id": "W92",
        "reason": "ReservedConcurrentExecutions not required"
    }
],
}

},
}

"Endpoint": {
    "Type": "AWS::CloudFormation::CustomResource",      => 사용자 지정 리소스를 지정
    "Properties": {
        "ServiceToken": {
            "Fn::GetAtt": [
                "CustomResource8CDCD7A7",
                "Arn"
            ]
        }
    }
},
```

Project – 5. Video On Demand

```
    ],
}

},
"UpdateReplacePolicy": "Delete",
"DeletionPolicy": "Delete",
"Metadata": {
    "aws:cdk:path": "VodFoundation/Endpoint/Default"
}
},
"jobSubmitServiceRole829286B1": {
    "Type": "AWS::IAM::Role",
    "Properties": {
        "AssumeRolePolicyDocument": {
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "lambda.amazonaws.com"
                    }
                }
            ],
            "Version": "2012-10-17"
        },
    }
},
```

Project – 5. Video On Demand

```
"ManagedPolicyArns": [  
    {  
        "Fn::Join": [  
            "",  
            [  
                "arn:",  
                {  
                    "Ref": "AWS::Partition"  
                },  
                ":iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"  
            ]  
        ]  
    },  
    {"  
        "Metadata": {  
            "aws:cdk:path": "VodFoundation/jobSubmit/ServiceRole/Resource"  
        }  
    },  
    {"  
        "jobSubmitServiceRoleDefaultPolicy": "EC39C00E",  
        "Type": "AWS::IAM::Policy",  
        "Properties": {  
            "PolicyDocument": {  
                "Statement": [  
                    {"Effect": "Allow",  
                    "Action": "lambda:InvokeFunction",  
                    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:JobSubmitFunction"}  
                ]  
            }  
        }  
    }  
],  
"Type": "AWS::IAM::Policy",  
"Properties": {  
    "PolicyDocument": {  
        "Statement": [  
            {"Effect": "Allow",  
            "Action": "lambda:InvokeFunction",  
            "Resource": "arn:aws:lambda:us-east-1:123456789012:function:JobSubmitFunction"}  
        ]  
    }  
},  
"Version": "2012-10-17",  
"Statement": [  
    {"Effect": "Allow",  
    "Action": "lambda:InvokeFunction",  
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:JobSubmitFunction"}  
]
```

=> 작업 제출 서비스 역할

기본정책

Project – 5. Video On Demand

```
"Statement": [  
    {  
        "Action": "iam:PassRole",  
                    => 사용자에게 AWS서비스 역할을 전달  
        "Effect": "Allow",  
        "Resource": {  
            "Fn::GetAtt": [  
                "MediaConvertRole031A64A9",  
                "Arn"  
            ]  
        }  
    },  
    {  
        "Action": "mediaconvert>CreateJob",  
                    => 미디어 변환 작업 생성  
        "Effect": "Allow",  
        "Resource": {  
            "Fn::Join": [  
                "",  
                [  
                    "arn:",  
                    {  
                        "Ref": "AWS::Partition"  
                    },  
                    ":mediaconvert:",  
                    {  
                        "Fn::Join": [  
                            "",  
                            [  
                                "arn:",  
                                {  
                                    "Ref": "AWS::Partition"  
                                },  
                                ":mediaconvert:  
                            ]  
                        ]  
                    }  
                ]  
            ]  
        }  
    }  
]
```

Project – 5. Video On Demand

```
    "Ref": "AWS::Region"
},
":",
{
    "Ref": "AWS::AccountId"
},
":*"
]
}
},
{
    "Action": "s3:GetObject",
    "Effect": "Allow",
    "Resource": [
        {
            "Fn::GetAtt": [
                "Source71E471F1",
                "Arn"
            ]
        },
        {
            "Fn::Join": [
                "",
                "
            ],
            "Fn::Sub": [
                "${AWS::Region}.*"
            ]
        }
    ]
}
```

Project – 5. Video On Demand

```
[  
 {  
   "Fn::GetAtt": [  
     "Source71E471F1",  
     "Arn"  
   ]  
 },  
 /*  
 ]  
 }  
 ]  
 },  
 {  
   "Action": "sns:Publish",  
   "Effect": "Allow",  
   "Resource": {  
     "Ref": "NotificationSnsTopicB941FD22"  
   }  
 }  
,  
 "Version": "2012-10-17"  
,  
 "PolicyName": "jobSubmitServiceRoleDefaultPolicyEC39C00E",  
 => SNS 게시
```

Project – 5. Video On Demand

```
"Roles": [  
  {  
    "Ref": "jobSubmitServiceRole829286B1"  
  },  
  ]  
,  
 "Metadata": {  
  "aws:cdk:path": "VodFoundation/jobSubmit/ServiceRole/DefaultPolicy/Resource"  
}  
,  
 "jobSubmitB391E42F": {  
  "Type": "AWS::Lambda::Function",  
  "Properties": {  
    "Code": {  
      "S3Bucket": {  
        "Fn::Sub": "solutions-#{AWS::Region}"  
      },  
      "S3Key": "video-on-demand-on-aws-  
foundation/v1.1.0/asset4c6b58d49775af65e43794635d2357ef117bab689af2d60c7838caf  
0ab3f3de.zip"  
    },  
    "Role": {  
      "Fn::GetAtt": [  
        "jobSubmitServiceRole829286B1",  
        "Arn"  
      ]  
    }  
  }  
},  
 "Fn::GetAtt": [  
  "jobSubmitServiceRole829286B1",  
  "Arn"  
]
```

Project – 5. Video On Demand

```
]

},
"Description": "Submits an Encoding job to MediaConvert",
"Environment": {
    "Variables": {
        "MEDIAconvert_ENDPOINT": {
            "Fn::GetAtt": [
                "Endpoint",
                "Endpoint"
            ]
        },
        "MEDIAconvert_ROLE": {
            "Fn::GetAtt": [
                "MediaConvertRole031A64A9",
                "Arn"
            ]
        },
        "JOB_SETTINGS": "job-settings.json",
        "DESTINATION_BUCKET": {
            "Ref": "Destination920A3C57"
        },
        "SOLUTION_ID": "SO0146",
        "STACKNAME": {
            "Ref": "AWS::StackName"
        }
    }
}
```

Project – 5. Video On Demand

```
},  
  "SOLUTION_IDENTIFIER": "AwsSolution/SO0146/v1.1.0",  
  "SNS_TOPIC_ARN": {  
    "Ref": "NotificationSnsTopicB941FD22"  
  },  
  "SNS_TOPIC_NAME": {  
    "Fn::GetAtt": [  
      "NotificationSnsTopicB941FD22",  
      "TopicName"  
    ]  
  }  
},  
  "Handler": "index.handler",  
  "Runtime": "nodejs12.x",  
  "Timeout": 30  
},  
  "DependsOn": [  
    "jobSubmitServiceRoleDefaultPolicyEC39C00E",  
    "jobSubmitServiceRole829286B1"  
],  
  "Metadata": {  
    "cfn_nag": {  
      "rules_to_suppress": [  
        "F2224",  
        "W3201",  
        "W3202",  
        "W3203",  
        "W3204",  
        "W3205",  
        "W3206",  
        "W3207",  
        "W3208",  
        "W3209",  
        "W3210",  
        "W3211",  
        "W3212",  
        "W3213",  
        "W3214",  
        "W3215",  
        "W3216",  
        "W3217",  
        "W3218",  
        "W3219",  
        "W3220",  
        "W3221",  
        "W3222",  
        "W3223",  
        "W3224",  
        "W3225",  
        "W3226",  
        "W3227",  
        "W3228",  
        "W3229",  
        "W3230",  
        "W3231",  
        "W3232",  
        "W3233",  
        "W3234",  
        "W3235",  
        "W3236",  
        "W3237",  
        "W3238",  
        "W3239",  
        "W3240",  
        "W3241",  
        "W3242",  
        "W3243",  
        "W3244",  
        "W3245",  
        "W3246",  
        "W3247",  
        "W3248",  
        "W3249",  
        "W3250",  
        "W3251",  
        "W3252",  
        "W3253",  
        "W3254",  
        "W3255",  
        "W3256",  
        "W3257",  
        "W3258",  
        "W3259",  
        "W3260",  
        "W3261",  
        "W3262",  
        "W3263",  
        "W3264",  
        "W3265",  
        "W3266",  
        "W3267",  
        "W3268",  
        "W3269",  
        "W3270",  
        "W3271",  
        "W3272",  
        "W3273",  
        "W3274",  
        "W3275",  
        "W3276",  
        "W3277",  
        "W3278",  
        "W3279",  
        "W3280",  
        "W3281",  
        "W3282",  
        "W3283",  
        "W3284",  
        "W3285",  
        "W3286",  
        "W3287",  
        "W3288",  
        "W3289",  
        "W3290",  
        "W3291",  
        "W3292",  
        "W3293",  
        "W3294",  
        "W3295",  
        "W3296",  
        "W3297",  
        "W3298",  
        "W3299",  
        "W32100",  
        "W32101",  
        "W32102",  
        "W32103",  
        "W32104",  
        "W32105",  
        "W32106",  
        "W32107",  
        "W32108",  
        "W32109",  
        "W32110",  
        "W32111",  
        "W32112",  
        "W32113",  
        "W32114",  
        "W32115",  
        "W32116",  
        "W32117",  
        "W32118",  
        "W32119",  
        "W32120",  
        "W32121",  
        "W32122",  
        "W32123",  
        "W32124",  
        "W32125",  
        "W32126",  
        "W32127",  
        "W32128",  
        "W32129",  
        "W32130",  
        "W32131",  
        "W32132",  
        "W32133",  
        "W32134",  
        "W32135",  
        "W32136",  
        "W32137",  
        "W32138",  
        "W32139",  
        "W32140",  
        "W32141",  
        "W32142",  
        "W32143",  
        "W32144",  
        "W32145",  
        "W32146",  
        "W32147",  
        "W32148",  
        "W32149",  
        "W32150",  
        "W32151",  
        "W32152",  
        "W32153",  
        "W32154",  
        "W32155",  
        "W32156",  
        "W32157",  
        "W32158",  
        "W32159",  
        "W32160",  
        "W32161",  
        "W32162",  
        "W32163",  
        "W32164",  
        "W32165",  
        "W32166",  
        "W32167",  
        "W32168",  
        "W32169",  
        "W32170",  
        "W32171",  
        "W32172",  
        "W32173",  
        "W32174",  
        "W32175",  
        "W32176",  
        "W32177",  
        "W32178",  
        "W32179",  
        "W32180",  
        "W32181",  
        "W32182",  
        "W32183",  
        "W32184",  
        "W32185",  
        "W32186",  
        "W32187",  
        "W32188",  
        "W32189",  
        "W32190",  
        "W32191",  
        "W32192",  
        "W32193",  
        "W32194",  
        "W32195",  
        "W32196",  
        "W32197",  
        "W32198",  
        "W32199",  
        "W32200",  
        "W32201",  
        "W32202",  
        "W32203",  
        "W32204",  
        "W32205",  
        "W32206",  
        "W32207",  
        "W32208",  
        "W32209",  
        "W32210",  
        "W32211",  
        "W32212",  
        "W32213",  
        "W32214",  
        "W32215",  
        "W32216",  
        "W32217",  
        "W32218",  
        "W32219",  
        "W32220",  
        "W32221",  
        "W32222",  
        "W32223",  
        "W32224",  
        "W32225",  
        "W32226",  
        "W32227",  
        "W32228",  
        "W32229",  
        "W32230",  
        "W32231",  
        "W32232",  
        "W32233",  
        "W32234",  
        "W32235",  
        "W32236",  
        "W32237",  
        "W32238",  
        "W32239",  
        "W32240",  
        "W32241",  
        "W32242",  
        "W32243",  
        "W32244",  
        "W32245",  
        "W32246",  
        "W32247",  
        "W32248",  
        "W32249",  
        "W32250",  
        "W32251",  
        "W32252",  
        "W32253",  
        "W32254",  
        "W32255",  
        "W32256",  
        "W32257",  
        "W32258",  
        "W32259",  
        "W32260",  
        "W32261",  
        "W32262",  
        "W32263",  
        "W32264",  
        "W32265",  
        "W32266",  
        "W32267",  
        "W32268",  
        "W32269",  
        "W32270",  
        "W32271",  
        "W32272",  
        "W32273",  
        "W32274",  
        "W32275",  
        "W32276",  
        "W32277",  
        "W32278",  
        "W32279",  
        "W32280",  
        "W32281",  
        "W32282",  
        "W32283",  
        "W32284",  
        "W32285",  
        "W32286",  
        "W32287",  
        "W32288",  
        "W32289",  
        "W32290",  
        "W32291",  
        "W32292",  
        "W32293",  
        "W32294",  
        "W32295",  
        "W32296",  
        "W32297",  
        "W32298",  
        "W32299",  
        "W322100",  
        "W322101",  
        "W322102",  
        "W322103",  
        "W322104",  
        "W322105",  
        "W322106",  
        "W322107",  
        "W322108",  
        "W322109",  
        "W322110",  
        "W322111",  
        "W322112",  
        "W322113",  
        "W322114",  
        "W322115",  
        "W322116",  
        "W322117",  
        "W322118",  
        "W322119",  
        "W322120",  
        "W322121",  
        "W322122",  
        "W322123",  
        "W322124",  
        "W322125",  
        "W322126",  
        "W322127",  
        "W322128",  
        "W322129",  
        "W322130",  
        "W322131",  
        "W322132",  
        "W322133",  
        "W322134",  
        "W322135",  
        "W322136",  
        "W322137",  
        "W322138",  
        "W322139",  
        "W322140",  
        "W322141",  
        "W322142",  
        "W322143",  
        "W322144",  
        "W322145",  
        "W322146",  
        "W322147",  
        "W322148",  
        "W322149",  
        "W322150",  
        "W322151",  
        "W322152",  
        "W322153",  
        "W322154",  
        "W322155",  
        "W322156",  
        "W322157",  
        "W322158",  
        "W322159",  
        "W322160",  
        "W322161",  
        "W322162",  
        "W322163",  
        "W322164",  
        "W322165",  
        "W322166",  
        "W322167",  
        "W322168",  
        "W322169",  
        "W322170",  
        "W322171",  
        "W322172",  
        "W322173",  
        "W322174",  
        "W322175",  
        "W322176",  
        "W322177",  
        "W322178",  
        "W322179",  
        "W322180",  
        "W322181",  
        "W322182",  
        "W322183",  
        "W322184",  
        "W322185",  
        "W322186",  
        "W322187",  
        "W322188",  
        "W322189",  
        "W322190",  
        "W322191",  
        "W322192",  
        "W322193",  
        "W322194",  
        "W322195",  
        "W322196",  
        "W322197",  
        "W322198",  
        "W322199",  
        "W322200",  
        "W322201",  
        "W322202",  
        "W322203",  
        "W322204",  
        "W322205",  
        "W322206",  
        "W322207",  
        "W322208",  
        "W322209",  
        "W322210",  
        "W322211",  
        "W322212",  
        "W322213",  
        "W322214",  
        "W322215",  
        "W322216",  
        "W322217",  
        "W322218",  
        "W322219",  
        "W322220",  
        "W322221",  
        "W322222",  
        "W322223",  
        "W322224",  
        "W322225",  
        "W322226",  
        "W322227",  
        "W322228",  
        "W322229",  
        "W322230",  
        "W322231",  
        "W322232",  
        "W322233",  
        "W322234",  
        "W322235",  
        "W322236",  
        "W322237",  
        "W322238",  
        "W322239",  
        "W322240",  
        "W322241",  
        "W322242",  
        "W322243",  
        "W322244",  
        "W322245",  
        "W322246",  
        "W322247",  
        "W322248",  
        "W322249",  
        "W322250",  
        "W322251",  
        "W322252",  
        "W322253",  
        "W322254",  
        "W322255",  
        "W322256",  
        "W322257",  
        "W322258",  
        "W322259",  
        "W322260",  
        "W322261",  
        "W322262",  
        "W322263",  
        "W322264",  
        "W322265",  
        "W322266",  
        "W322267",  
        "W322268",  
        "W322269",  
        "W322270",  
        "W322271",  
        "W322272",  
        "W322273",  
        "W322274",  
        "W322275",  
        "W322276",  
        "W322277",  
        "W322278",  
        "W322279",  
        "W322280",  
        "W322281",  
        "W322282",  
        "W322283",  
        "W322284",  
        "W322285",  
        "W322286",  
        "W322287",  
        "W322288",  
        "W322289",  
        "W322290",  
        "W322291",  
        "W322292",  
        "W322293",  
        "W322294",  
        "W322295",  
        "W322296",  
        "W322297",  
        "W322298",  
        "W322299",  
        "W322300",  
        "W322301",  
        "W322302",  
        "W322303",  
        "W322304",  
        "W322305",  
        "W322306",  
        "W322307",  
        "W322308",  
        "W322309",  
        "W322310",  
        "W322311",  
        "W322312",  
        "W322313",  
        "W322314",  
        "W322315",  
        "W322316",  
        "W322317",  
        "W322318",  
        "W322319",  
        "W322320",  
        "W322321",  
        "W322322",  
        "W322323",  
        "W322324",  
        "W322325",  
        "W322326",  
        "W322327",  
        "W322328",  
        "W322329",  
        "W322330",  
        "W322331",  
        "W322332",  
        "W322333",  
        "W322334",  
        "W322335",  
        "W322336",  
        "W322337",  
        "W322338",  
        "W322339",  
        "W322340",  
        "W322341",  
        "W322342",  
        "W322343",  
        "W322344",  
        "W322345",  
        "W322346",  
        "W322347",  
        "W322348",  
        "W322349",  
        "W322350",  
        "W322351",  
        "W322352",  
        "W322353",  
        "W322354",  
        "W322355",  
        "W322356",  
        "W322357",  
        "W322358",  
        "W322359",  
        "W322360",  
        "W322361",  
        "W322362",  
        "W322363",  
        "W322364",  
        "W322365",  
        "W322366",  
        "W322367",  
        "W322368",  
        "W322369",  
        "W322370",  
        "W322371",  
        "W322372",  
        "W322373",  
        "W322374",  
        "W322375",  
        "W322376",  
        "W322377",  
        "W322378",  
        "W322379",  
        "W322380",  
        "W322381",  
        "W322382",  
        "W322383",  
        "W322384",  
        "W322385",  
        "W322386",  
        "W322387",  
        "W322388",  
        "W322389",  
        "W322390",  
        "W322391",  
        "W322392",  
        "W322393",  
        "W322394",  
        "W322395",  
        "W322396",  
        "W322397",  
        "W322398",  
        "W322399",  
        "W322400",  
        "W322401",  
        "W322402",  
        "W322403",  
        "W322404",  
        "W322405",  
        "W322406",  
        "W322407",  
        "W322408",  
        "W322409",  
        "W322410",  
        "W322411",  
        "W322412",  
        "W322413",  
        "W322414",  
        "W322415",  
        "W322416",  
        "W322417",  
        "W322418",  
        "W322419",  
        "W322420",  
        "W322421",  
        "W322422",  
        "W322423",  
        "W322424",  
        "W322425",  
        "W322426",  
        "W322427",  
        "W322428",  
        "W322429",  
        "W322430",  
        "W322431",  
        "W322432",  
        "W322433",  
        "W322434",  
        "W322435",  
        "W322436",  
        "W322437",  
        "W322438",  
        "W322439",  
        "W322440",  
        "W322441",  
        "W322442",  
        "W322443",  
        "W322444",  
        "W322445",  
        "W322446",  
        "W322447",  
        "W322448",  
        "W322449",  
        "W322450",  
        "W322451",  
        "W322452",  
        "W322453",  
        "W322454",  
        "W322455",  
        "W322456",  
        "W322457",  
        "W322458",  
        "W322459",  
        "W322460",  
        "W322461",  
        "W322462",  
        "W322463",  
        "W322464",  
        "W322465",  
        "W322466",  
        "W322467",  
        "W322468",  
        "W322469",  
        "W322470",  
        "W322471",  
        "W322472",  
        "W322473",  
        "W322474",  
        "W322475",  
        "W322476",  
        "W322477",  
        "W322478",  
        "W322479",  
        "W322480",  
        "W322481",  
        "W322482",  
        "W322483",  
        "W322484",  
        "W322485",  
        "W322486",  
        "W322487",  
        "W322488",  
        "W322489",  
        "W322490",  
        "W322491",  
        "W322492",  
        "W322493",  
        "W322494",  
        "W322495",  
        "W322496",  
        "W322497",  
        "W322498",  
        "W322499",  
        "W322500",  
        "W322501",  
        "W322502",  
        "W322503",  
        "W322504",  
        "W322505",  
        "W322506",  
        "W322507",  
        "W322508",  
        "W322509",  
        "W322510",  
        "W322511",  
        "W322512",  
        "W322513",  
        "W322514",  
        "W322515",  
        "W322516",  
        "W322517",  
        "W322518",  
        "W322519",  
        "W322520",  
        "W322521",  
        "W322522",  
        "W322523",  
        "W322524",  
        "W322525",  
        "W322526",  
        "W322527",  
        "W322528",  
        "W322529",  
        "W322530",  
        "W322531",  
        "W322532",  
        "W322533",  
        "W322534",  
        "W322535",  
        "W322536",  
        "W322537",  
        "W322538",  
        "W322539",  
        "W322540",  
        "W322541",  
        "W322542",  
        "W322543",  
        "W322544",  
        "W322545",  
        "W322546",  
        "W322547",  
        "W322548",  
        "W322549",  
        "W322550",  
        "W322551",  
        "W322552",  
        "W322553",  
        "W322554",  
        "W322555",  
        "W322556",  
        "W322557",  
        "W322558",  
        "W322559",  
        "W322560",  
        "W322561",  
        "W322562",  
        "W322563",  
        "W322564",  
        "W322565",  
        "W322566",  
        "W322567",  
        "W322568",  
        "W322569",  
        "W322570",  
        "W322571",  
        "W322572",  
        "W322573",  
        "W322574",  
        "W322575",  
        "W322576",  
        "W322577",  
        "W322578",  
        "W322579",  
        "W322580",  
        "W322581",  
        "W322582",  
        "W322583",  
        "W322584",  
        "W322585",  
        "W322586",  
        "W322587",  
        "W322588",  
        "W322589",  
        "W322590",  
        "W322591",  
        "W322592",  
        "W322593",  
        "W322594",  
        "W322595",  
        "W322596",  
        "W322597",  
        "W322598",  
        "W322599",  
        "W322600",  
        "W322601",  
        "W322602",  
        "W322603",  
        "W322604",  
        "W322605",  
        "W322606",  
        "W322607",  
        "W322608",  
        "W322609",  
        "W322610",  
        "W322611",  
        "W322612",  
        "W322613",  
        "W322614",  
        "W322615",  
        "W322616",  
        "W322617",  
        "W322618",  
        "W322619",  
        "W322620",  
        "W322621",  
        "W322622",  
        "W322623",  
        "W322624",  
        "W322625",  
        "W322626",  
        "W322627",  
        "W322628",  
        "W322629",  
        "W322630",  
        "W322631",  
        "W322632",  
        "W322633",  
        "W322634",  
        "W322635",  
        "W322636",  
        "W322637",  
        "W322638",  
        "W322639",  
        "W322640",  
        "W322641",  
        "W322642",  
        "W322643",  
        "W322644",  
        "W322645",  
        "W322646",  
        "W322647",  
        "W322648",  
        "W322649",  
        "W322650",  
        "W322651",  
        "W322652",  
        "W322653",  
        "W322654",  
        "W322655",  
        "W322656",  
        "W322657",  
        "W322658",  
        "W322659",  
        "W322660",  
        "W322661",  
        "W322662",  
        "W322663",  
        "W322664",  
        "W322665",  
        "W322666",<
```

Project – 5. Video On Demand

```
{  
    "id": "W58",  
    "reason": "Invalid warning: function has access to cloudwatch"  
,  
{  
    "id": "W89",  
    "reason": "AWS Lambda does not require VPC for this solution."  
,  
{  
    "id": "W92",  
    "reason": "ReservedConcurrentExecutions not required"  
}  
]  
}  
},  
"jobSubmitEventInvokeConfig0385F502": {  
    "Type": "AWS::Lambda::EventInvokeConfig",  
    "Properties": {  
        "FunctionName": {  
            "Ref": "jobSubmitB391E42F"  
        },  
        "Qualifier": "$LATEST",  
        "MaximumRetryAttempts": 0  
    }  
}
```

=> 람다 비동기 호출

Project – 5. Video On Demand

```
},  
  "Metadata": {  
    "aws:cdk:path": "VodFoundation/jobSubmit/EventInvokeConfig/Resource"  
  }  
,  
  "jobSubmitS3Trigger3DEB8D7C": {  
    "Type": "AWS::Lambda::Permission",  
    "Properties": {  
      "Action": "lambda:InvokeFunction",  
      "FunctionName": {  
        "Fn::GetAtt": [  
          "jobSubmitB391E42F",  
          "Arn"  
        ]  
      },  
      "Principal": "s3.amazonaws.com",  
      "SourceAccount": {  
        "Ref": "AWS::AccountId"  
      }  
,  
      "Metadata": {  
        "aws:cdk:path": "VodFoundation/jobSubmit/S3Trigger"  
      }  
,  
    }  
},
```

Project – 5. Video On Demand

```
"JobCompleteServiceRole2855C268": {  
    "Type": "AWS::IAM::Role",  
    "Properties": {  
        "AssumeRolePolicyDocument": {  
            "Statement": [  
                {  
                    "Action": "sts:AssumeRole",  
                    "Effect": "Allow",  
                    "Principal": {  
                        "Service": "lambda.amazonaws.com"  
                    }  
                }  
            ],  
            "Version": "2012-10-17"  
        },  
        "ManagedPolicyArns": [  
            {  
                "Fn::Join": [  
                    "",  
                    [  
                        "arn:",  
                        {  
                            "Ref": "AWS::Partition"  
                        },  
                        {"  
                        }  
                    ]  
                ]  
            }  
        ]  
    }  
}
```

Project – 5. Video On Demand

```
":iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"

]

}

]

},

"Metadata": {

    "aws:cdk:path": "VodFoundation/JobComplete/ServiceRole/Resource"
}

},

"JobCompleteServiceRoleDefaultPolicy686BE0F5": {

    "Type": "AWS::IAM::Policy",

    "Properties": {

        "PolicyDocument": {

            "Statement": [

                {

                    "Action": "mediaconvert:GetJob",           => 미디어 변환 작업 가져오기

                    "Effect": "Allow",

                    "Resource": {

                        "Fn::Join": [
                            "",

                            [
                                "arn:",
                                {

```

Project – 5. Video On Demand

```
"Ref": "AWS::Partition"
},
":mediaconvert:",
{
"Ref": "AWS::Region"
},
":",
{
"Ref": "AWS::AccountId"
},
":",
":*"
]
]
}
},
{
"Action": [
"s3:GetObject",
"s3:PutObject"
],
"Effect": "Allow",
"Resource": {
"Fn::Join": [
"" ,
"
```

Project – 5. Video On Demand

```
[  
 {  
 "Fn::GetAtt": [  
 "Source71E471F1",  
 "Arn"  
 ],  
 },  
 /*  
 ]  
 }  
,  
 {  
 "Action": "sns:Publish",  
 "Effect": "Allow",  
 "Resource": {  
 "Ref": "NotificationSnsTopicB941FD22"  
 }  
 }  
,  
 "Version": "2012-10-17"  
 },  
 "PolicyName": "JobCompleteServiceRoleDefaultPolicy686BE0F5",  
 "Roles": [
```

Project – 5. Video On Demand

```
{  
    "Ref": "JobCompleteServiceRole2855C268"  
}  
]  
,  
"Metadata": {  
    "aws:cdk:path": "VodFoundation/JobComplete/ServiceRole/DefaultPolicy/Resource"  
}  
},  
"JobComplete703682D0": {  
    "Type": "AWS::Lambda::Function",  
    "Properties": {  
        "Code": {  
            "S3Bucket": {  
                "Fn::Sub": "solutions-${AWS::Region}"  
            },  
            "S3Key": "video-on-demand-on-aws-  
foundation/v1.1.0/asset2030979b01f18577476da5df8ca758912810df394a1bd22127da4e1  
807693998.zip"  
        },  
        "Role": {  
            "Fn::GetAtt": [  
                "JobCompleteServiceRole2855C268",  
                "Arn"  
            ]  
        }  
    }  
}
```

Project – 5. Video On Demand

```
},  
  
"Description": "Triggered by Cloudwatch Events,processes completed MediaConvert  
jobs.",  
  
"Environment": {  
  
    "Variables": {  
  
        "MEDIAconvert_ENDPOINT": {=> 미디어 컨벌트 엔드포인트  
            "Fn::GetAtt": [  
  
                "Endpoint",  
  
                "Endpoint"  
  
            ]  
  
        },  
  
        "CLOUDFRONT_DOMAIN": {=> 클라우드 프론트 도메인  
            "Fn::GetAtt": [  
  
                "CloudFrontCloudFrontDistribution824F3346",  
  
                "DomainName"  
  
            ]  
  
        },  
  
        "SOURCE_BUCKET": {=> 소스 버킷  
            "Ref": "Source71E471F1"  
  
        },  
  
        "JOB_MANIFEST": "jobs-manifest.json",  
  
        "STACKNAME": {  
  
            "Ref": "AWS::StackName"  
  
        },  
  
        "METRICS": {
```

Project – 5. Video On Demand

```
"Fn::FindInMap": [  
    "Send",  
    "AnonymousUsage",  
    "Data"  
,  
    "]  
,  
  "SOLUTION_ID": "SO0146",  
  "VERSION": "1.1.0",  
  "UUID": {  
    "Fn::GetAtt": [  
      "Endpoint",  
      "UUID"  
,  
      "]  
,  
    "SOLUTION_IDENTIFIER": "AwsSolution/SO0146/v1.1.0",  
    "SNS_TOPIC_ARN": {  
      "Ref": "NotificationSnsTopicB941FD22"  
,  
      "SNS_TOPIC_NAME": {  
        "Fn::GetAtt": [  
          "NotificationSnsTopicB941FD22",  
          "TopicName"  
,  
          "]  
,  
        "}  
    }  
}
```

Project – 5. Video On Demand

```
    },
    "Handler": "index.handler",
    "Runtime": "nodejs12.x",
    "Timeout": 30
},
"DependsOn": [
    "JobCompleteServiceRoleDefaultPolicy686BE0F5",
    "JobCompleteServiceRole2855C268"
],
"Metadata": {
    "cfn_nag": {
        "rules_to_suppress": [
            {
                "id": "W58",
                "reason": "Invalid warning: function has access to cloudwatch"
            },
            {
                "id": "W89",
                "reason": "AWS Lambda does not require VPC for this solution."
            },
            {
                "id": "W92",
                "reason": "ReservedConcurrentExecutions not required"
            }
        ]
    }
}
```

Project – 5. Video On Demand

```
    }

    ]

}

},


"JobCompleteEventInvokeConfig692D89BE": {

    "Type": "AWS::Lambda::EventInvokeConfig",

    "Properties": {

        "FunctionName": {

            "Ref": "JobComplete703682D0"

        },

        "Qualifier": "$LATEST",

        "MaximumRetryAttempts": 0

    },

    "Metadata": {

        "aws:cdk:path": "VodFoundation/JobComplete/EventInvokeConfig/Resource"

    }

},


"JobCompleteAwsEventsLambdaInvokePermission1ED79B615": {

    "Type": "AWS::Lambda::Permission",

    "Properties": {

        "Action": "lambda:InvokeFunction",

        "FunctionName": {

            "Fn::GetAtt": [


```

Project – 5. Video On Demand

```
"JobComplete703682D0",
"Arn"
],
},
"Principal": "events.amazonaws.com",
"SourceArn": {
"Fn::GetAtt": [
"EventTriggerEventsRule76A88FDF",
"Arn"
]
}
},
"Metadata": {
"aws:cdk:path": "VodFoundation/JobComplete/AwsEventsLambdaInvokePermission-1"
}
},
"S3Config": {
>Type": "AWS::CloudFormation::CustomResource",
"Properties": {
"ServiceToken": {
"Fn::GetAtt": [
"CustomResource8CDCD7A7",
"Arn"
]
}
```

Project – 5. Video On Demand

Project – 5. Video On Demand

```
"aws.mediaconvert"

],
"detail": {
    "userMetadata": {
        "StackName": [
            {
                "Ref": "AWS::StackName"
            }
        ]
    },
    "status": [
        "COMPLETE",
        "ERROR",
        "CANCELED",
        "INPUT_INFORMATION"
    ]
},
"State": "ENABLED",
"Targets": [
{
    "Arn": {
        "Fn::GetAtt": [
            "JobComplete703682D0",

```

Project – 5. Video On Demand

```
        "Arn":  
    ]  
},  
    "Id": "Target0"  
}  
]  
,  
"Metadata": {  
    "aws:cdk:path": "VodFoundation/EventTrigger/EventsRule/Resource"  
}  
,  
"NotificationSnsTopicB941FD22": {  
    "Type": "AWS::SNS::Topic",  
    "Properties": {  
        "KmsMasterKeyId": {  
            "Fn::Join": [  
                "",  
                [  
                    "arn:",  
                    {  
                        "Ref": "AWS::Partition"  
                    },  
                    ":kms:",  
                    {

```

Project – 5. Video On Demand

```
"Ref": "AWS::Region"

},
":",
{

"Ref": "AWS::AccountId"

},
":alias/aws/sns"

]

}

"Metadata": {

"aws:cdk:path": "VodFoundation/Notification/SnsTopic/Resource"

}

},
"NotificationSnsTopicPolicy4027082A": {

"Type": "AWS::SNS::TopicPolicy",

"Properties": {

"PolicyDocument": {

"Statement": [

{

"Action": [

"SNS:Publish",

"SNS:RemovePermission",

```

Project – 5. Video On Demand

```
"SNS:SetTopicAttributes",
"SNS>DeleteTopic",
"SNS>ListSubscriptionsByTopic",
"SNS>GetTopicAttributes",
"SNS>Receive",
"SNS>AddPermission",
"SNS>Subscribe"
],
"Condition": {
  "StringEquals": {
    "AWS:SourceOwner": {
      "Ref": "AWS::AccountId"
    }
  }
},
"Effect": "Allow",
"Principal": {
  "AWS": {
    "Fn::Join": [
      "",
      [
        "arn:",
        {
          "Ref": "AWS::Partition"
        }
      ]
    ]
  }
}
```

Project – 5. Video On Demand

```
    },
    ":iam::",
    {
        "Ref": "AWS::AccountId"
    },
    ":root"
]
}
},
"Resource": {
    "Ref": "NotificationSnsTopicB941FD22"
},
{
    "Sid": "TopicOwnerOnlyAccess"
},
{
    "Action": [
        "SNS:Publish",
        "SNS:RemovePermission",
        "SNS:SetTopicAttributes",
        "SNS:DeleteTopic",
        "SNS>ListSubscriptionsByTopic",
        "SNS:GetTopicAttributes",
        "SNS:Receive",
    ]
}
```

Project – 5. Video On Demand

```
"SNS:AddPermission",
"SNS:Subscribe"
],
"Condition": {
"Bool": {
"aws:SecureTransport": "false"
}
},
"Effect": "Deny",
"Principal": "*",
"Resource": {
"Ref": "NotificationSnsTopicB941FD22"
},
"Sid": "HttpsOnly"          => https 만 허용, http 액세스 거부
},
],
"Version": "2012-10-17"
},
"Topics": [
{
"Ref": "NotificationSnsTopicB941FD22"
}
]
},
```

Project – 5. Video On Demand

```
"Metadata": {  
    "aws:cdk:path": "VodFoundation/Notification/SnsTopic/Policy/Resource"  
}  
,  
"NotificationSnsTopicTokenSubscription1209F3ABA": {  
    "Type": "AWS::SNS::Subscription",  
    "Properties": {  
        "Protocol": "email",  
        "TopicArn": {  
            "Ref": "NotificationSnsTopicB941FD22"  
        },  
        "Endpoint": {  
            "Ref": "emailAddress"  
        }  
    },  
    "Metadata": {  
        "aws:cdk:path":  
        "VodFoundation/Notification/SnsTopic/TokenSubscription:1/Resource"  
    }  
,  
    "CDKMetadata": {  
        "Type": "AWS::CDK::Metadata",  
        "Properties": {  
            "Analytics":  
                =>  
                분석  
"v2:deflate64:H4sIAAAAAAAA3VSwW7CMAz9Fu5poKu084ANCWkTCPiBkBoU2iZVnDBNVf9
```

Project – 5. Video On Demand

```
9TlJoD9ultl/sl+eX5jzPF3wxexPfmHWyrOadNBZ4d3RCVmxB0V+ibZW+hnQvrGjAgWVro9FZL  
x1bloKj5mvs8ehMcwA03k0ll898Cu68a70LGfGUyimjexYFYMG7IZcVxNMhS2FvaiV/RnioU7ES  
CD2TtfHlxRtePeuSKA6+0DOdlaRvqWUgLgtQTvlltM6DGzCwH8dU5qeKdHw7mDqtFql06qU9  
awWzbkUvNt4LePlPbMP+5EvdV3UwGtfIHR1j/BPdhGlcZrschEsBl5dJtBGEBS4gclFKILE3QyrZ  
IBS0n8jhqn5dGfUVrVPjRO674nOlPHrTGTj8fGefpLnjZn9F6jhydzLAZtmSVJ2WBF3A+DyJP5jN  
BgUhYkJ4RmNdKt2pTAbzi/5y88f+X57IZKERs9SAP8kOlvl5symLUCAAA="
```

```
},
```

```
"Metadata": {
```

```
    "aws:cdk:path": "VodFoundation/CDKMetadata/Default"
```

```
},
```

```
    "Condition": "CDKMetadataAvailable"
```

```
}
```

```
},
```

```
"Outputs": {
```

```
    "SourceBucket": {
```

```
        "Description": "Source S3 Bucket used to host source video and MediaConvert job  
settings files",
```

```
        "Value": {
```

```
            "Ref": "Source71E471F1"
```

```
        },
```

```
        "Export": {
```

```
            "Name": {
```

```
                "Fn::Join": [
```

```
                    "",
```

```
                    [
```

```
                        {
```

Project – 5. Video On Demand

```
        "Ref": "AWS::StackName"  
    },  
    "-SourceBucket"  
]  
]  
}  
},  
}  
],  
}  
},  
"  
"DestinationBucket": {  
    "Description": "Source S3 Bucket used to host all MediaConvert ouputs",  
    "Value": {  
        "Ref": "Destination920A3C57"  
    },  
    "Export": {  
        "Name": {  
            "Fn::Join": [  
                "",  
                [  
                    {  
                        "Ref": "AWS::StackName"  
                    },  
                    "-DestinationBucket"  
                ]  
            ]  
        }  
    }  
}
```

Project – 5. Video On Demand

```
    },
    },
},
"CloudFrontDomain": {
    "Description": "CloudFront Domain Name",
    "Value": {
        "Fn::GetAtt": [
            "CloudFrontCloudFrontDistribution824F3346",
            "DomainName"
        ]
    },
    "Export": {
        "Name": {
            "Fn::Join": [
                "",
                [
                    {
                        "Ref": "AWS::StackName"
                    },
                    "-CloudFrontDomain"
                ]
            ]
        }
    }
}
```

Project – 5. Video On Demand

```
},  
  "SnsTopic": {  
    "Description": "SNS Topic used to capture the VOD workflow outputs including errors",  
    "Value": {  
      "Fn::GetAtt": [  
        "NotificationSnsTopicB941FD22",  
        "TopicName"  
      ]  
    },  
    "Export": {  
      "Name": {  
        "Fn::Join": [  
          "",  
          [  
            {"  
              "Ref": "AWS::StackName"  
            },  
            "-SnsTopic"  
          ]  
        ]  
      },  
      "  
    }  
  },  
},
```

Project – 5. Video On Demand

```
"Conditions": {  
    "CDKMetadataAvailable": {  
        "Fn::Or": [  
            {  
                "Fn::Or": [  
                    {  
                        "Fn::Equals": [  
                            {  
                                "Ref": "AWS::Region"  
                            },  
                            "af-south-1"  
                        ]  
                    },  
                    {  
                        "Fn::Equals": [  
                            {  
                                "Ref": "AWS::Region"  
                            },  
                            "ap-east-1"  
                        ]  
                    },  
                    {  
                        "Fn::Equals": [  
                            {  
                                "Ref": "AWS::Region"  
                            },  
                            "sa-east-1"  
                        ]  
                    }  
                ]  
            }  
        ]  
    }  
}
```

Project – 5. Video On Demand

```
"Ref": "AWS::Region"  
},  
"ap-northeast-1"  
]  
,  
{  
"Fn::Equals": [  
{  
"Ref": "AWS::Region"  
},  
"ap-northeast-2"  
]  
,  
{  
"Fn::Equals": [  
{  
"Ref": "AWS::Region"  
},  
"ap-south-1"  
]  
,  
{  
"Fn::Equals": [  
{
```

Project – 5. Video On Demand

```
"Ref": "AWS::Region"  
},  
"ap-southeast-1"  
]  
,  
{  
"Fn::Equals": [  
{  
"Ref": "AWS::Region"  
},  
"ap-southeast-2"  
]  
,  
{  
"Fn::Equals": [  
{  
"Ref": "AWS::Region"  
},  
"ca-central-1"  
]  
,  
{  
"Fn::Equals": [  
{
```

Project – 5. Video On Demand

```
"Ref": "AWS::Region"  
},  
"cn-north-1"  
]  
,  
{  
"Fn::Equals": [  
{  
"Ref": "AWS::Region"  
},  
"cn-northwest-1"  
]  
}  
]  
,  
{  
"Fn::Or": [  
{  
"Fn::Equals": [  
{  
"Ref": "AWS::Region"  
},  
"eu-central-1"  
]  
}
```

Project – 5. Video On Demand

```
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "eu-north-1"  
    ]  
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "eu-south-1"  
    ]  
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "eu-west-1"  
    ]  
}
```

Project – 5. Video On Demand

```
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "eu-west-2"  
    ]  
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "eu-west-3"  
    ]  
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "me-south-1"  
    ]  
}
```

Project – 5. Video On Demand

```
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "sa-east-1"  
    ]  
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "us-east-1"  
    ]  
},  
{  
    "Fn::Equals": [  
        {  
            "Ref": "AWS::Region"  
        },  
        "us-east-2"  
    ]  
}
```

Project – 5. Video On Demand

```
    },
],
},
{
  "Fn::Or": [
    {
      "Fn::Equals": [
        {
          "Ref": "AWS::Region"
        },
        "us-west-1"
      ]
    },
    {
      "Fn::Equals": [
        {
          "Ref": "AWS::Region"
        },
        "us-west-2"
      ]
    }
  ]
}
```

```
    }  
}  
}
```

6. Ansible

- Ansible Server : Bastion Host (Bastion Host 2에서도 동일하게 진행)
- Ansible Client : Web Server 1 , Web Server 2
- ansible 패키지 설치는 2. CloudFormation의 UserData를 통해 진행
- 관리자 권한이 필요하므로 sudo 명령어를 사용하여 진행

1) Ansible Server – Bastion Host

- 설정파일 편집

```
# sudo vi /etc/ansible/ansible.cfg  
host_key_checking = False
```

- PlayBook 생성

```
# sudo vi playbook_ly.yaml
```

```
  - hosts: all  
    become: true  
    become_method: sudo  
    gather_facts: no
```

tasks :

```
- name: Lynis security audit playbook (install)
  yum: name=lynis state=present

- name: Audit Scan the system
  shell: sudo lynis audit system > /tmp/lynis-output.log

- name: Downloading report locally
  fetch:
    src: "/tmp/lynis-output.log"
    dest: "./tmp/{{ inventory_hostname }}-lynis-output.log"
    flat: yes
```

1) Ansible Client – Web Server 1 , Web Server 2 동일하게 진행

- Ansible Server에서 배포한 스크립트의 결과가 다시 Server로 돌아올 수 있도록
Client에서도 설정을 해야함

- elp 레포지토리 생성확인 & 서비스 버전 업그레이드

```
# sudo yum -y update
# sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-
7.noarch.rpm
```

```
# sudo ssh -i ./server1.pem ec2-user@10.5.50.14
```

```
10.5.50.34/
```

```
10.5.100.65
```

3) Ansible Server에서 스크립트 배포 후 결과 확인

- ping Test를 통해 연결 확인

```
# sudo ansible all -m ping -i ~/.ansible/inventory
```

- PlayBook 배포

```
# sudo ansible-playbook ./playbook_ly.yaml -i ~/.ansible/inventory
```

```
[ec2-user@ip-10-5-20-41 ~]$ sudo ansible-playbook ./playbook_ly.yaml -i ~/.ansible/inventory
PLAY [all] ****
TASK [Lynis security audit playbook (install)] ****
[WARNING]: Platform linux on host 10.5.100.65 is using the discovered Python interpreter at /usr/bin/python,
but future installation of another Python interpreter could change this. See
https://docs.ansible.com/ansible/2.9/reference_appendices/interpreter_discovery.html for more information.
changed: [10.5.100.65]
[WARNING]: Platform linux on host 10.5.50.34 is using the discovered Python interpreter at /usr/bin/python, but
future installation of another Python interpreter could change this. See
https://docs.ansible.com/ansible/2.9/reference_appendices/interpreter_discovery.html for more information.
changed: [10.5.50.34]

TASK [Audit Scan the system] ****
changed: [10.5.100.65]
changed: [10.5.50.34]

TASK [Downloading report locally] ****
changed: [10.5.100.65]
changed: [10.5.50.34]

PLAY RECAP ****
10.5.100.65 : ok=3    changed=3    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.5.50.34   : ok=3    changed=3    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Security Check

- Client로부터 전달 받은 스크립트 결과 확인

```
# sudo vi ./tmp/Web1-lynis-output.log
```

```
^[[1;37m[ Lynis 3.0.6 ]^[[0m
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISOfy - https://cisofty.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] ^[[1;33mInitializing program^[[0m
-----
^[[2C- Detecting OS... ^[[41C [ ^[[1;32mDONE^[[0m ]
^[[2C- Checking profiles...^[[37C [ ^[[1;32mDONE^[[0m ]

-----
Program version: 3.0.6
Operating system: Linux
Operating system name: Amazon Linux
Operating system version: 2
Kernel version: 4.14.248
"Web1-lynis-output.log" [readonly] 680L, 32877C
```

Log file

7. Zabbix Server

1) 레포지토리 설정

```
# sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

```
# sudo tee /etc/yum.repos.d/mariadb.repo<<EOF
```

```
[mariadb]
```

```
name = MariaDB
```

```
baseurl = http://yum.mariadb.org/10.5/centos7-amd64
```

```
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
```

```
gpgcheck=1
```

```
EOF
```

2) 마리아 DB 설치 및 설정

```
# sudo yum -y install MariaDB-server MariaDB-client
```

```
# sudo systemctl enable mariadb
```

```
# sudo systemctl start mariadb
```

```
# sudo mysql_secure_installation
```

```
# mysql -u root -p
```

```
CREATE DATABASE zabbix CHARACTER SET utf8 COLLATE utf8_bin;
```

```
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'P@ssword';
```

```
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
```

```
FLUSH PRIVILEGES;
```

```
EXIT
```

3) 아파치 설치 및 설정

```
# sudo yum -y install httpd vim bash-completion
```

```
# sudo systemctl enable httpd
```

```
# sudo systemctl start httpd
```

```
# sudo vi /etc/httpd/conf/httpd.conf
```

```
ServerName zabbix.example.com
```

```
# sudo vi /etc/httpd/conf/httpd.conf
```

```
ServerAdmin admin@example.com
```

```
# sudo systemctl restart httpd
```

4) Zabbix Server 설치

```
# sudo yum -y install https://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-release-5.0-1.el7.noarch.rpm
```

```
# sudo yum -y install zabbix-server-mysql zabbix-agent zabbix-get
```

```
# sudo tee /etc/yum.repos.d/centos-scl.repo<<EOF
```

```
[centos-sclo-sclo]
```

```
name=CentOS-7 - SCLo sclo
```

```
baseurl=http://mirror.centos.org/centos/7/scl/x86_64/scl/
```

```
gpgcheck=0
```

```
enabled=1
```

```
[centos-sclo-rh]

name=CentOS-7 - SCLo rh

baseurl=http://mirror.centos.org/centos/7/sclo/x86_64/rh/

gpgcheck=0

enabled=1

EOF
```

```
# sudo yum makecache

# sudo yum-config-manager --enable zabbix-frontend

# sudo yum -y install zabbix-web-mysql-scl zabbix-apache-conf-scl
```

5) Zabbix Server 설정

```
# sudo zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -
p'P@ssword' zabbix
```

```
# sudo systemctl start zabbix-server zabbix-agent

# sudo systemctl enable zabbix-server zabbix-agent
```

```
# sudo vi /etc/zabbix/zabbix_server.conf
```

```
DBHost=localhost
```

```
DBName=zabbix
```

```
DBUser=zabbix
```

```
DBPassword=P@ssword
```

Project – 7. Zabbix Server

```
# sudo vi /etc/opt/rh/rh-php72/php-fpm.d/zabbix.conf  
php_value[date.timezone] = Asia/Seoul
```

```
# sudo systemctl restart zabbix-server zabbix-agent httpd rh-php72-php-fpm  
# sudo systemctl enable zabbix-server zabbix-agent httpd rh-php72-php-fpm
```

5) Zabbix Server Web 설정



- 설치 가능 확인 (OK 확인하고 Next)

	Current value	Required	Status
PHP version	7.2.24	7.2.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	Asia/Seoul		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK

Project – 7. Zabbix Server

- 데이터베이스 연결

ZABBIX

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install

Database type: MySQL
Database host: localhost
Database port: 0 (0 - use default port)
Database name: zabbix
User: zabbix
Password:

Database TLS encryption: Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).

[Back](#) [Next step](#)

ZABBIX

Pre-installation summary

Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install

Database type: MySQL
Database server: localhost
Database port: default
Database name: zabbix
Database user: zabbix
Database password:
Database TLS encryption: false

Zabbix server: localhost
Zabbix server port: 10051
Zabbix server name:

[Back](#) [Next step](#)

ZABBIX

Install

Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install

Congratulations! You have successfully installed Zabbix frontend.
Configuration file "/etc/zabbix/web/zabbix.conf.php" created.

[Back](#) [Finish](#)

8. Zabbix Agent

1) Zabbix Agent 설치

```
# sudo rpm -ivh http://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-agent-5.0.3-1.el7.x86_64.rpm
```

```
# sudo yum localinstall http://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-agent-5.0.3-1.el7.x86_64.rpm
```

2) Zabbix Agent 설정

```
# sudo systemctl enable zabbix-agent.service
```

```
# sudo systemctl start zabbix-agent.service
```

3) Zabbix Port 설정

- AWS 콘솔에서 포트 인바운드 허용하기

Server ← 10051/TCP ← Agent

Server → 10050/TCP → Agent

인바운드 규칙		아웃바운드 규칙		태그
유형	프로토콜	포트 범위	소스	설명 - 선택 사항
사용자 지정 TCP	TCP	10050		For Zabbix Server to Polling Data
사용자 지정 TCP	TCP	10050		For Zabbix Server to Polling Data

Project – 8. Zabbix Agent

4) Zabbix Port 확인

- Bastion 서버에서 작업

```
# sudo yum install -y nc
```

```
nc -v -z 10.5.50.34 10050
```

5) Zabbix Agent 추가

The screenshot shows two pages of the Zabbix web interface.

Top Page (Hosts List):

- Left sidebar: Monitoring, Inventory, Reports, Configuration (Host groups, Templates, Hosts, Maintenance, Actions, Event correlation, Discovery, Services), Administration, Support.
- Header: ZABBIX, Hosts, Create host.
- Search bar: type here to search.
- Filters: Host groups, Templates, Name, DNS, IP, Port, Monitored by (Any, Server, Proxy), Tags (And/Or, Or), Proxy, Status, Availability, Agent encryption.
- Table: Shows two hosts:
 - Web Server 1: IP 10.5.50.34:10050, Status Enabled, Monitored by ZBX|SNMP|JMX|IPMI, Agent encryption NONE.
 - Zabbix server: IP 127.0.0.1:10050, Status Enabled, Monitored by ZBX|SNMP|JMX|IPMI, Agent encryption NONE.
- Buttons: Apply, Reset, Display.

Bottom Page (Create Host Form):

- Left sidebar: same as the top page.
- Header: ZABBIX, Hosts.
- Form fields:
 - Host name: Web Server 1.
 - Visible name: (empty).
 - Groups: web (new) (with a remove button).
 - Interfaces:
 - Type: Agent, IP address: 10.5.50.34, DNS name: (empty), Connect to: IP, Port: 10050, Default checked.
 - Description: (empty).
 - Monitored by proxy: (no proxy).
 - Enabled: checked.
- Buttons: Add, Cancel.

	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent enc	
<input type="checkbox"/>	Web Server 1	Applications	Items	Triggers	Graphs	Discovery	Web	10.5.50.34: 10050			Enabled	[ZBX SNMP JMX IPMI]	NONE	
<input type="checkbox"/>	Web Server 2	Applications	Items	Triggers	Graphs	Discovery	Web	10.5.100.65: 10050			Enabled	[ZBX SNMP JMX IPMI]	NONE	
<input type="checkbox"/>	Zabbix server	Applications 12	Items 89	Triggers 49	Graphs 18	Discovery 3	Web 127.0.0.1: 10050		Template App Zabbix Server, Template OS Linux by Zabbix agent (Template Module Linux block devices by Zabbix agent, Template Module Linux CPU by Zabbix agent, Template Module Linux filesystems by Zabbix agent, Template Module Linux generic by Zabbix agent, Template Module Linux memory by Zabbix agent, Template Module Linux network interfaces by Zabbix agent, Template Module Zabbix agent)			Enabled	[ZBX SNMP JMX IPMI]	NONE

Displ:

THANK YOU!

