|  |
| --- |
|  |
| 모듈프로젝트3 메뉴얼 |
|  |
|  |
| **김민지** |
|  |
|  |

|  |
| --- |
|  |

# 목차

[모듈프로젝트3 메뉴얼 0](#_Toc84255209)

[목차 1](#_Toc84255210)

[1. 프로젝트 요구사항 4](#_Toc84255211)

[1.1 외부(고객용) 시스템 4](#_Toc84255212)

[1.2 내부(직원용) CRM 시스템 4](#_Toc84255213)

[1.3 내부(직원용) Groupware 시스템 5](#_Toc84255214)

[2. 프로젝트 Architecture 6](#_Toc84255215)

[3. 프로젝트 예상 비용 7](#_Toc84255216)

[4 SSL 인증서 발급 9](#_Toc84255217)

[4.1 Certificate Manager 9](#_Toc84255222)

[4.1.1 인증서 9](#_Toc84255223)

[5 외부(고객용) 인프라 구성 10](#_Toc84255224)

[5.1 VPC 10](#_Toc84255228)

[5.1.1 VPC 10](#_Toc84255229)

[5.1.2 서브넷 11](#_Toc84255230)

[5.1.3 인터넷 게이트웨이 13](#_Toc84255231)

[5.1.4 탄력적 IP 주소 14](#_Toc84255232)

[5.1.5 NAT 게이트웨이 15](#_Toc84255233)

[5.1.6 라우팅 테이블 16](#_Toc84255234)

[5.1.7 네트워크 ACL 17](#_Toc84255235)

[5.1.8 보안 그룹 19](#_Toc84255236)

[5.1.9 네트워크 방화벽 규칙 그룹 21](#_Toc84255237)

[5.1.10 네트워크 방화벽 정책 22](#_Toc84255238)

[5.1.11 네트워크 방화벽 23](#_Toc84255239)

[5.2 bank-external-edge- subntet-01 24](#_Toc84255240)

[5.2.1 키페어 24](#_Toc84255241)

[5.2.2 인스턴스 24](#_Toc84255242)

[5.3 bank-external-web- subntet-01 25](#_Toc84255243)

[5.3.1 AMI 25](#_Toc84255244)

[5.3.2 키페어 26](#_Toc84255245)

[5.3.3 시작 템플릿 26](#_Toc84255246)

[5.3.4 Auto Scaling 그룹 27](#_Toc84255247)

[5.3.5 대상 그룹 28](#_Toc84255248)

[5.3.6 로드밸런서 28](#_Toc84255249)

[5.4 bank-external-was- subntet-01 30](#_Toc84255250)

[5.4.1 AMI 30](#_Toc84255251)

[5.4.2 키페어 32](#_Toc84255252)

[5.4.3 시작 템플릿 32](#_Toc84255253)

[5.4.4 Auto Scaling 그룹 33](#_Toc84255254)

[5.4.5 대상 그룹 33](#_Toc84255255)

[5.4.6 로드밸런서 35](#_Toc84255256)

[5.5 Route53 36](#_Toc84255257)

[5.5.1 호스팅 영역 36](#_Toc84255258)

[5.6 WAF & Shield 38](#_Toc84255259)

[5.6.1 Web ACLs 38](#_Toc84255260)

[5.7 bank-external-db-subntet-01 & bank-external-db-subntet-02 39](#_Toc84255261)

[5.7.1 서브넷 그룹 39](#_Toc84255262)

[5.7.2 데이터베이스 40](#_Toc84255263)

[6 내부(직원용) 인프라 구성 41](#_Toc84255264)

[6.1 VPC 41](#_Toc84255265)

[6.1.1 VPC 41](#_Toc84255266)

[6.1.2 서브넷 42](#_Toc84255267)

[6.1.3 인터넷 게이트웨이 44](#_Toc84255268)

[6.1.4 탄력적 IP 주소 45](#_Toc84255269)

[6.1.5 NAT 게이트웨이 47](#_Toc84255270)

[6.1.6 라우팅 테이블 48](#_Toc84255271)

[6.1.7 네트워크 ACL 49](#_Toc84255272)

[6.1.8 보안 그룹 51](#_Toc84255273)

[6.1.9 네트워크 방화벽 규칙 그룹 53](#_Toc84255274)

[6.1.10 네트워크 방화벽 정책 54](#_Toc84255275)

[6.1.11 네트워크 방화벽 55](#_Toc84255276)

[6.2 bank-internal-edge- subntet-01 56](#_Toc84255277)

[6.2.1 키페어 56](#_Toc84255278)

[6.2.2 인스턴스 56](#_Toc84255279)

[6.3 bank-internal-web- subntet-01 58](#_Toc84255280)

[6.3.1 AMI 58](#_Toc84255281)

[6.3.2 키페어 61](#_Toc84255282)

[6.3.3 시작 템플릿 61](#_Toc84255283)

[6.3.4 Auto Scaling 그룹 62](#_Toc84255284)

[6.3.5 대상 그룹 63](#_Toc84255285)

[6.3.6 로드밸런서 64](#_Toc84255286)

[6.4 bank-internal-was- subntet-01 66](#_Toc84255287)

[6.4.1 AMI 66](#_Toc84255288)

[6.4.2 키페어 69](#_Toc84255289)

[6.4.3 시작 템플릿 69](#_Toc84255290)

[6.4.4 Auto Scaling 그룹 70](#_Toc84255291)

[6.4.5 대상 그룹 71](#_Toc84255292)

[6.4.6 로드밸런서 72](#_Toc84255293)

[6.5 Route53 73](#_Toc84255294)

[6.5.1 호스팅 영역 73](#_Toc84255295)

[6.6 WAF & Shield 75](#_Toc84255296)

[6.6.1 Web ACLs 75](#_Toc84255297)

[6.7 bank-internal-db-subntet-01 & bank-internal-db-subntet-02 76](#_Toc84255298)

[6.7.1 서브넷 그룹 76](#_Toc84255299)

[6.7.2 데이터베이스 77](#_Toc84255300)

[7 구성하면서 발생했던 오류 79](#_Toc84255301)

[8 구성하면서 알게된 점 80](#_Toc84255302)

[9 추가 실습(모듈프로젝트2 + AWS 연동) 81](#_Toc84255303)

[10 향후 과제 82](#_Toc84255304)

# 프로젝트 요구사항

## 외부(고객용) 시스템

* Web: CPU 2 / Memory 8 / Linux (Nginx) / 150대
* WAS: CPU 4 / Memory 32 / Linux (Flask) / 100대
* DB: CPU 32 / Memory 256 / MySQL과 호환되는 Amazon Aurora / 1대 / 10TB
* 3 Tier 구성 / Web: 443 -> WAS: 5001 -> DB: 3309
* Cloud Watch / Cloud Trail
* 사이트 간 VPN 연결 (Site-to-site VPN) / 피어링 연결 -> 내부(직원): 개발 / 엔지니어 / 보안

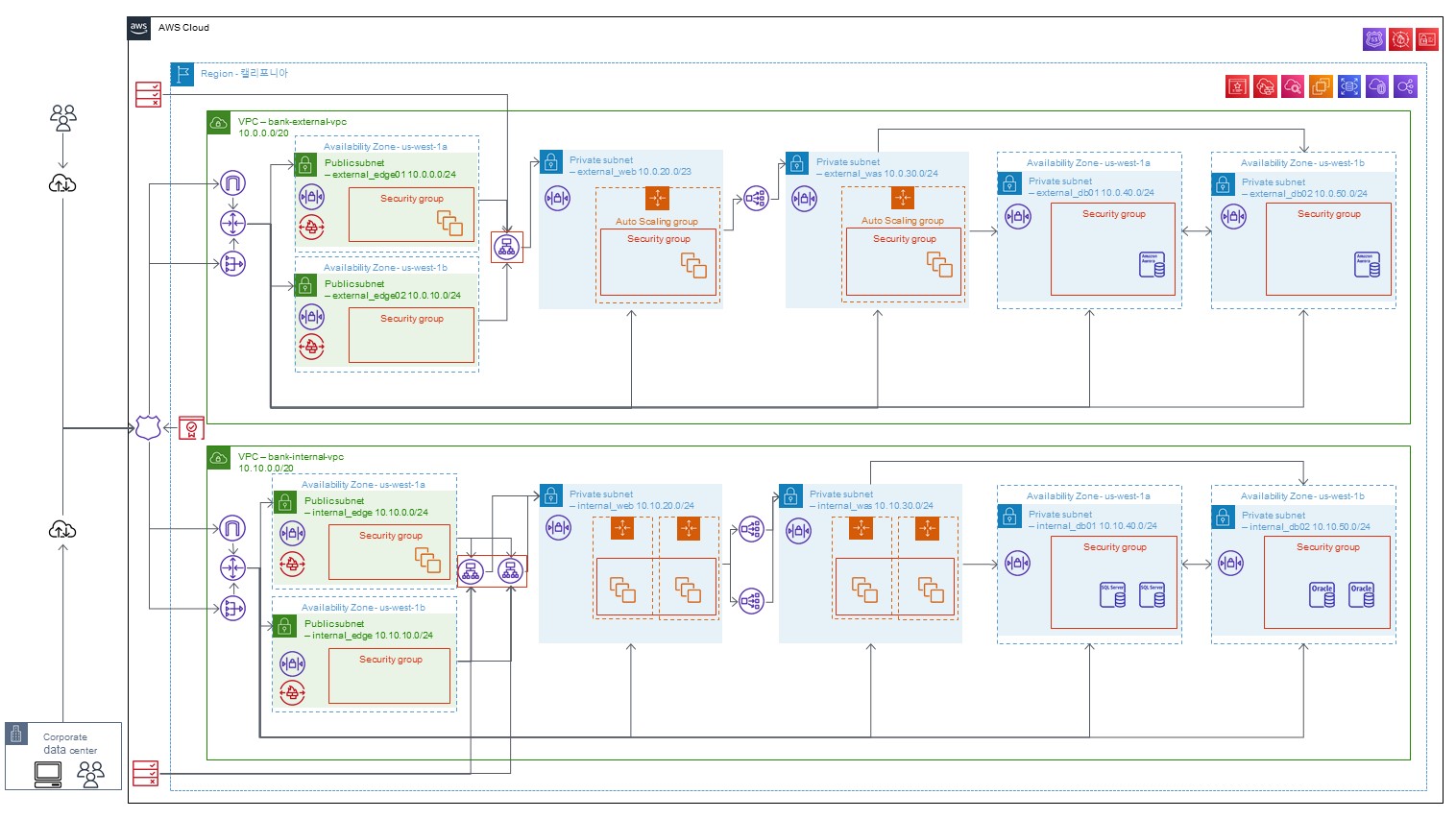
## 내부(직원용) CRM 시스템

* Web: CPU 4 / Memory 16 / Linux + Docker (Nginx) / 100대
* WAS: CPU 16 / Memory 64 / Linux + Docker (Flask) / 50대
* DB: CPU 32 / Memory 128 / Oracle / 1대 / 10TB
* 3 Tier 구성 / Web: 443 -> WAS: 5001 -> DB: 1521
* Cloud Watch / Cloud Trail
* 사이트 간 VPN 연결 (Site-to-site VPN)

## 내부(직원용) Groupware 시스템

* Web: CPU 2 / Memory 8 / Windows + Windows 기반 컨테이너 (IIS) / 20대
* WAS: CPU 8 / Memory 64 / Windows + Windows 기반 컨테이너 (Flask) / 10대
* DB: CPU 32 / Memory 128 / MS SQL / 1대 / 10TB
* 3 Tier 구성 / Web: 443 -> WAS: 5001 -> DB: 1455
* Cloud Watch / Cloud Trail
* 사이트 간 VPN 연결 (Site-to-site VPN)

# 프로젝트 Architecture



* 피어링 연결 / 사이트 간 VPN 연결 (Site-to-site VPN) / Cloud Trail 제외

# 프로젝트 예상 비용

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 리전 | 설명 | 서비스 | 선결제 | 월별 | 처음 12개월 합계 | 통화 |
| US West (N. California) | VPC | Amazon Virtual Private Cloud (VPC) | 0 | 0.81 | 9.72 | USD |
| DT 인바운드: Internet (10 월별 TB), DT 아웃바운드: Internet (10 월별 GB), DT 리전 내: (0 월별 TB) | | | | | | |
| US West (N. California) | NAT 게이트웨이 | Amazon Virtual Private Cloud (VPC) | 0 | 355.2 | 4262.4 | USD |
| NAT 게이트웨이 수 (10) | | | | | | |
| US West (N. California) | ex\_web | Amazon EC2 | 0 | 8838.293576 | 106059.52 | USD |
| 운영 체제 (Linux), 스토리지 크기 (8 GB), DT 인바운드: Internet (10 월별 TB), DT 아웃바운드: Internet (10 월별 GB), DT 리전 내: (10 월별 GB), 워크로드 (Weekly, 기준선: 75, 피크: 150, 피크 기간: 5 일 0 Hr 0 Min), 고급 EC2 인스턴스 (t2.large), Pricing strategy (EC2 Instance Savings Plans 1yr No Upfront), 스냅샷 빈도 (스냅샷 스토리지 없음) | | | | | | |
| US West (N. California) | ex\_was | Amazon EC2 | 0 | 16521.4 | 198256.8 | USD |
| 운영 체제 (Linux), 스토리지 크기 (8 GB), DT 인바운드: 기타 모든 리전 (10 월별 GB), DT 아웃바운드: 기타 모든 리전 (10 월별 GB), DT 리전 내: (10 월별 GB), 워크로드 (Weekly, 기준선: 50, 피크: 100, 피크 기간: 5 일 0 Hr 0 Min), 스냅샷 빈도 (스냅샷 스토리지 없음), 고급 EC2 인스턴스 (t3a.2xlarge), Pricing strategy (EC2 Instance Savings Plans 1yr No Upfront) | | | | | | |
| US West (N. California) | ex\_db | Amazon Aurora MySQL-Compatible | 0 | 1215.34 | 14584.08 | USD |
| 문당 레코드 변경 (0.38), 노드 (1), 인스턴스 유형 (db.t2.medium), 인스턴스 패밀리 (General purpose), 요금 모델 (OnDemand), 스토리지 크기 (10 TB) | | | | | | |
| US West (N. California) | in\_crm\_web | Amazon EC2 | 0 | 11698.11144 | 140377.34 | USD |
| 운영 체제 (Linux), 스토리지 크기 (8 GB), DT 인바운드: Internet (10 월별 TB), DT 아웃바운드: Internet (10 월별 GB), DT 리전 내: (10 월별 GB), 워크로드 (Weekly, 기준선: 50, 피크: 100, 피크 기간: 5 일 0 Hr 0 Min), 고급 EC2 인스턴스 (t2.xlarge), Pricing strategy (EC2 Instance Savings Plans 1yr No Upfront), 스냅샷 빈도 (스냅샷 스토리지 없음) | | | | | | |
| US West (N. California) | in\_crm\_was | Amazon EC2 | 0 | 24660.27859 | 295923.34 | USD |
| 운영 체제 (Linux), 스토리지 크기 (8 GB), DT 인바운드: 기타 모든 리전 (10 월별 TB), DT 아웃바운드: 기타 모든 리전 (10 월별 GB), DT 리전 내: (10 월별 GB), 워크로드 (Weekly, 기준선: 25, 피크: 50, 피크 기간: 5 일 0 Hr 0 Min), 고급 EC2 인스턴스 (m4.4xlarge), Pricing strategy (EC2 Instance Savings Plans 1yr No Upfront), 스냅샷 빈도 (스냅샷 스토리지 없음) | | | | | | |
| US West (N. California) | in\_crm\_db | Amazon RDS for Oracle | 0 | 7381.44 | 88577.28 | USD |
| 각 RDS 인스턴스의 스토리지 (범용 SSD(gp2)), 스토리지 크기 (10 TB), 노드 수 (1), 인스턴스 유형 (db.m5.8xlarge), 배포 옵션 (Multi-AZ), 요금 모델 (OnDemand), 라이선스 (Bring your own license), 데이터베이스 에디션 (Enterprise) | | | | | | |
| US West (N. California) | in\_groupware\_web | Amazon EC2 | 0 | 1574.957141 | 18899.49 | USD |
| 운영 체제 (Windows Server), 스토리지 크기 (30 GB), DT 인바운드: Internet (10 월별 TB), DT 아웃바운드: Internet (10 월별 GB), DT 리전 내: (10 월별 GB), 워크로드 (Weekly, 기준선: 10, 피크: 20, 피크 기간: 5 일 0 Hr 0 Min), 스냅샷 빈도 (스냅샷 스토리지 없음), 고급 EC2 인스턴스 (t2.large), Pricing strategy (EC2 Instance Savings Plans 1yr No Upfront) | | | | | | |
| US West (N. California) | in\_groupware\_was | Amazon EC2 | 0 | 5082.328611 | 60987.94 | USD |
| 운영 체제 (Windows Server), 스토리지 크기 (30 GB), DT 인바운드: 기타 모든 리전 (10 월별 TB), DT 아웃바운드: 기타 모든 리전 (10 월별 GB), DT 리전 내: (10 월별 GB), 워크로드 (Weekly, 기준선: 5, 피크: 10, 피크 기간: 5 일 0 Hr 0 Min), 고급 EC2 인스턴스 (r5.2xlarge), Pricing strategy (EC2 Instance Savings Plans 1yr No Upfront), 스냅샷 빈도 (스냅샷 스토리지 없음) | | | | | | |
| US West (N. California) | in\_groupware\_db | Amazon RDS for SQL server | 0 | 22955.26 | 275463.12 | USD |
| 각 RDS 인스턴스의 스토리지 (범용 SSD(gp2)), 스토리지 크기 (10 TB), 노드 수 (1), 인스턴스 유형 (db.m5.8xlarge), 배포 옵션 (Multi-AZ), 요금 모델 (OnDemand), 라이선스 (License included), 데이터베이스 에디션 (Enterprise) | | | | | | |
| US West (N. California) | ex\_alb | Application Load Balancer | 0 | 310.4 | 3724.8 | USD |
| Application Load Balancer 수 (1) | | | | | | |
| US West (N. California) | ex\_nlb | Network Load Balancer | 0 | 62.2 | 746.4 | USD |
| Network Load Balancer 수 (1), 평균 새 TCP 연결 수 (500 초당), TCP에 대한 NLB당 처리된 바이트 수 (10 GB 기준 시간), 평균 TCP 연결 기간 (5 분) | | | | | | |
| US West (N. California) | in\_alb | Application Load Balancer | 0 | 620.79 | 7449.48 | USD |
| Application Load Balancer 수 (2) | | | | | | |
| US West (N. California) | in\_nlb | Network Load Balancer | 0 | 124.39 | 1492.68 | USD |
| Network Load Balancer 수 (2), TCP에 대한 NLB당 처리된 바이트 수 (10 GB 기준 시간), 평균 새 TCP 연결 수 (500 초당), 평균 TCP 연결 기간 (5 분) | | | | | | |
| US West (N. California) | route 53 | Amazon Route 53 | 0 | 509 | 6108 | USD |
| 호스팅 영역 (10) | | | | | | |
| US West (N. California) | waf | AWS Web Application Firewall (WAF) | 0 | 21.6 | 259.2 | USD |
| 사용된 웹 ACL(액세스 제어 목록) 수 (1 월별), 웹 ACL당 추가된 규칙 수 (7 월별), 웹 ACL당 규칙 그룹 수 (1 월별), 각 규칙 그룹 내 규칙 수 (7 월별), 관리형 규칙 그룹 수 (1 월별) | | | | | | |
| US West (N. California) | eip | Amazon Elastic IP | 0 | 0.05 | 0.6 | USD |
| EC2 인스턴스 수 (10), 인스턴스당 EIP 수 (1) | | | | | | |
| US West (N. California) | cloud watch | Amazon CloudWatch | 0 | 3.0004 | 36 | USD |
| 지표 수(세부 및 사용자 지정 지표 포함) (10), GetMetricData: 요청된 지표 수 (10), GetMetricWidgetImage: 요청된 지표 수 (10), 다른 API 요청 수입니다. (10) | | | | | | |

* 선결제 비용: 0.00 USD / 월별 비용: 101,934.85 USD / 총 12개월 비용: 1,223,218.20 USD(약 14억 5000만 원)
* 피어링 연결 / 사이트 간 VPN 연결 (Site-to-site VPN) / Cloud Trail 제외

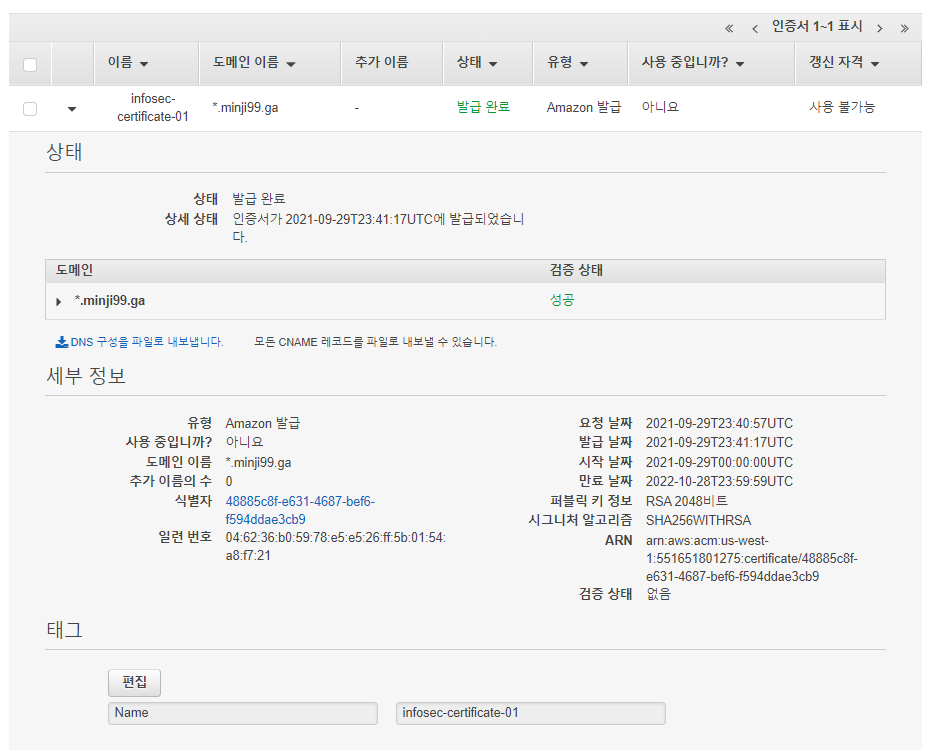
# SSL 인증서 발급



## Certificate Manager

### 인증서

|  |  |  |  |
| --- | --- | --- | --- |
| **인증서 이름** | **도메인 이름** | **상태** | **유형** |
| infosec-certificate-01 | \*.minji99.ga | 발급 완료 | Amazon 발급 |



# 외부(고객용) 인프라 구성



## VPC

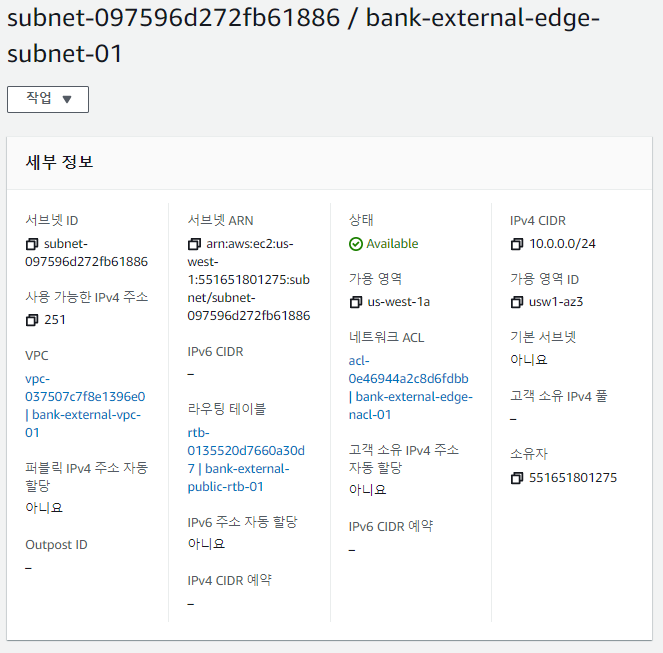
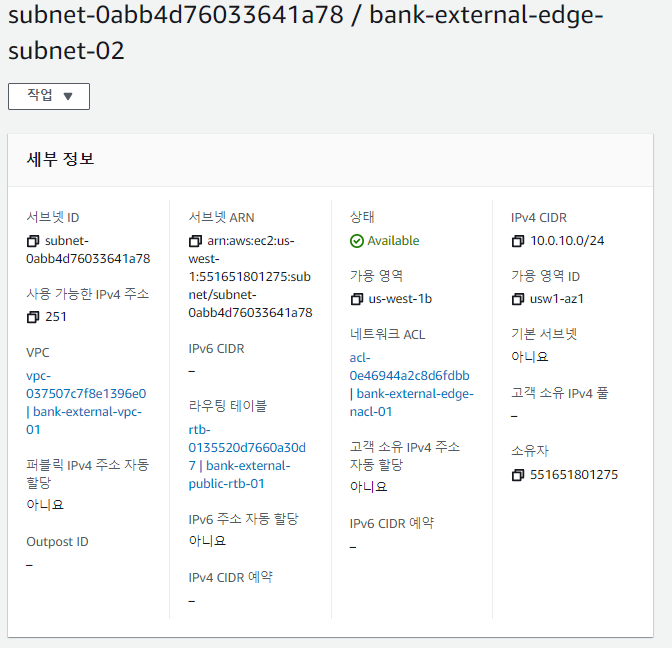
### VPC

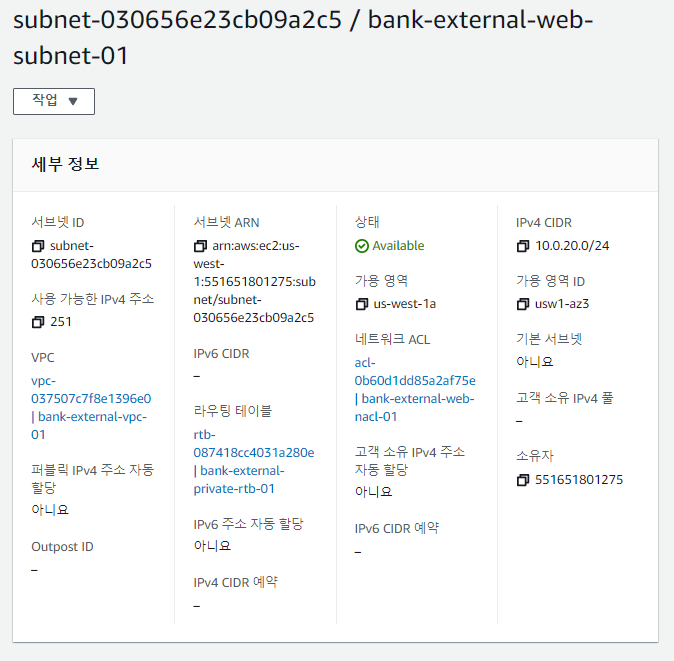
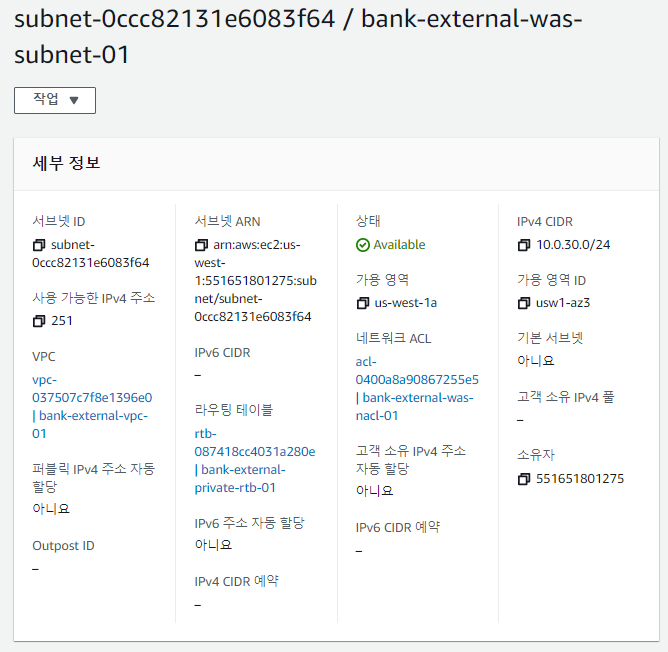
|  |  |
| --- | --- |
| **IP(CIDR)** | **VPC 이름** |
| 10.0.0.0/16 | bank-external-vpc-01 |

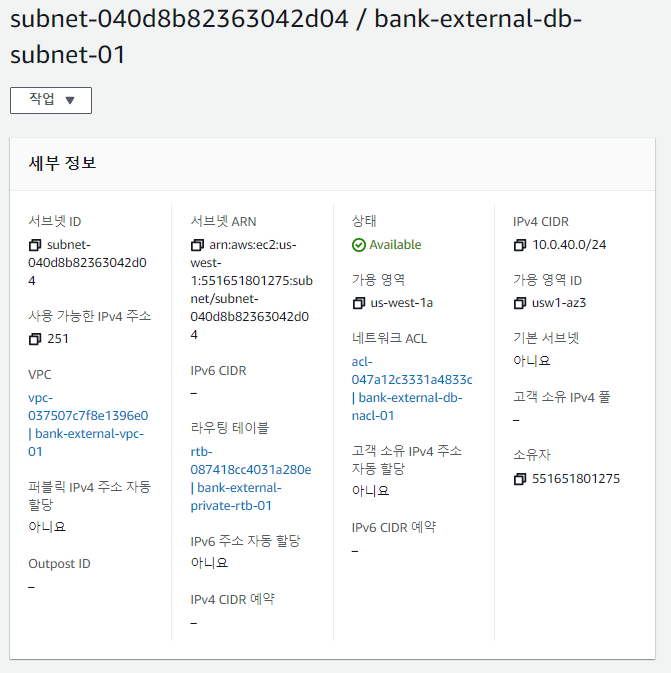
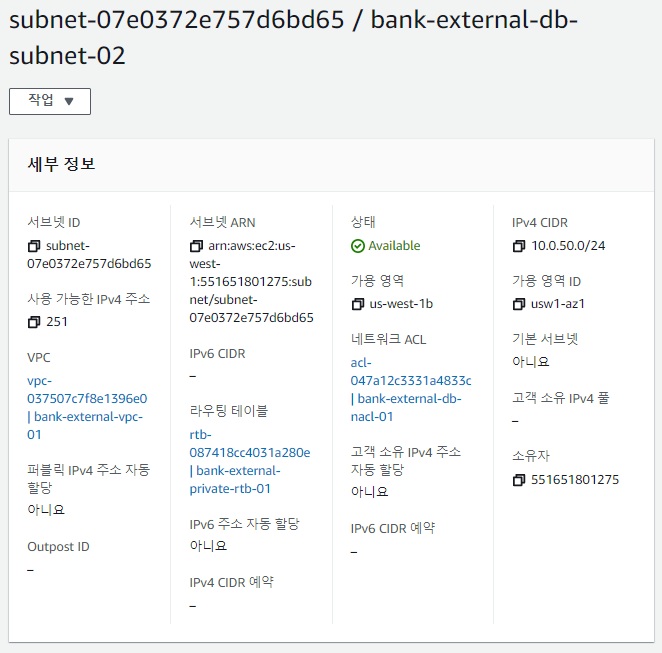


### 서브넷

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP(CIDR)** | **서브넷 이름** | **가용영역** | **가용영역 ID** | **VPC 이름** |
| 10.0.0.0/24 | bank-external-edge-subnet-01 | us-west-1a | usw1-az3 | bank-external-vpc-01 |
| 10.0.10.0/24 | bank-external-edge-subnet-02 | us-west-1b | usw1-az1 | bank-external-vpc-01 |
| 10.0.20.0/24 | bank-external-web-subnet-01 | us-west-1a | usw1-az3 | bank-external-vpc-01 |
| 10.0.30.0/24 | bank-external-was-subnet-01 | us-west-1a | usw1-az3 | bank-external-vpc-01 |
| 10.0.40.0/24 | bank-external-db-subnet-01 | us-west-1a | usw1-az3 | bank-external-vpc-01 |
| 10.0.50.0/24 | bank-external-db-subnet-02 | us-west-1b | usw1-az1 | bank-external-vpc-01 |

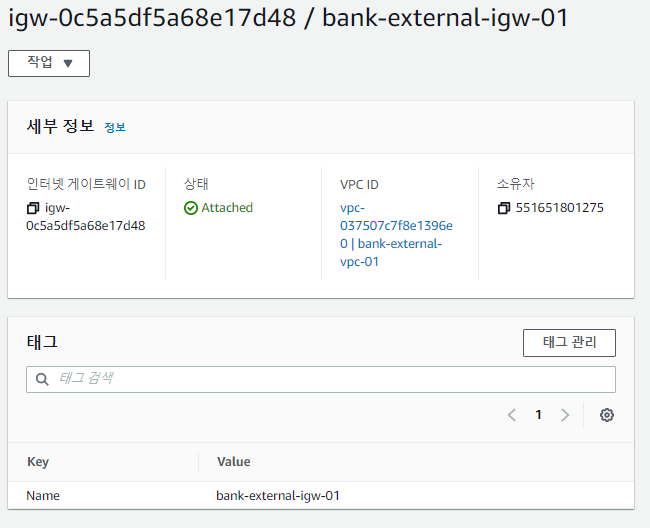
 

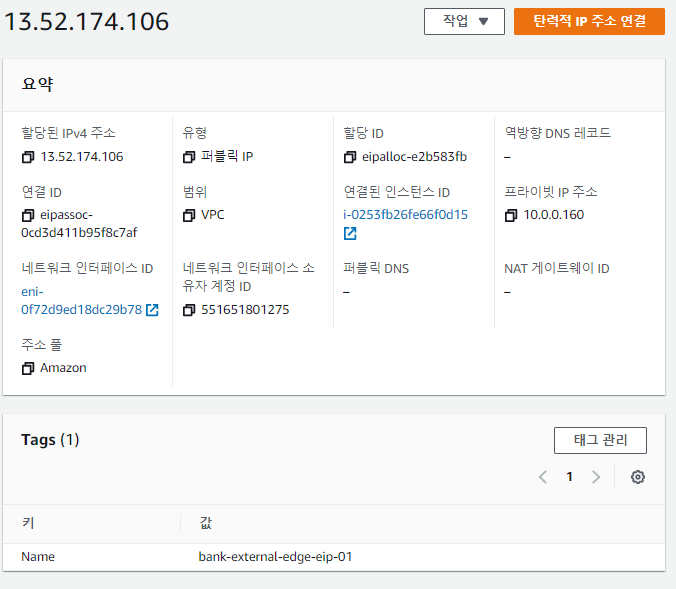
### 인터넷 게이트웨이

|  |  |
| --- | --- |
| **인터넷 게이트웨이 이름** | **VPC** 이름 |
| bank-external-igw-01 | bank-external-vpc-01 |



### 탄력적 IP 주소

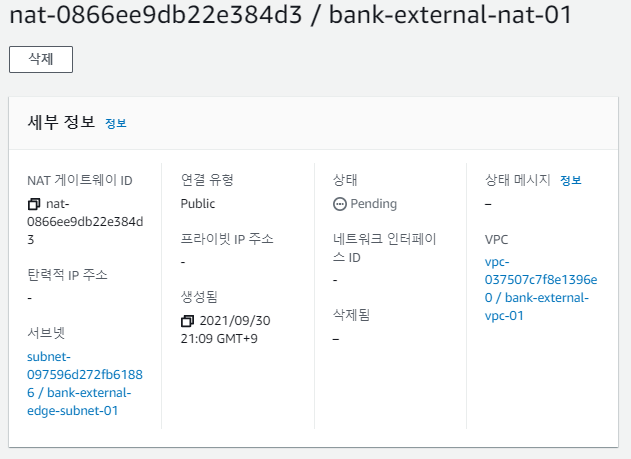
|  |
| --- |
| **탄력적 IP 주소 이름** |
| bank-external-edge-eip-01 |
| bank-external-edge-eip-02 |
| bank-external-nat-eip-01 |



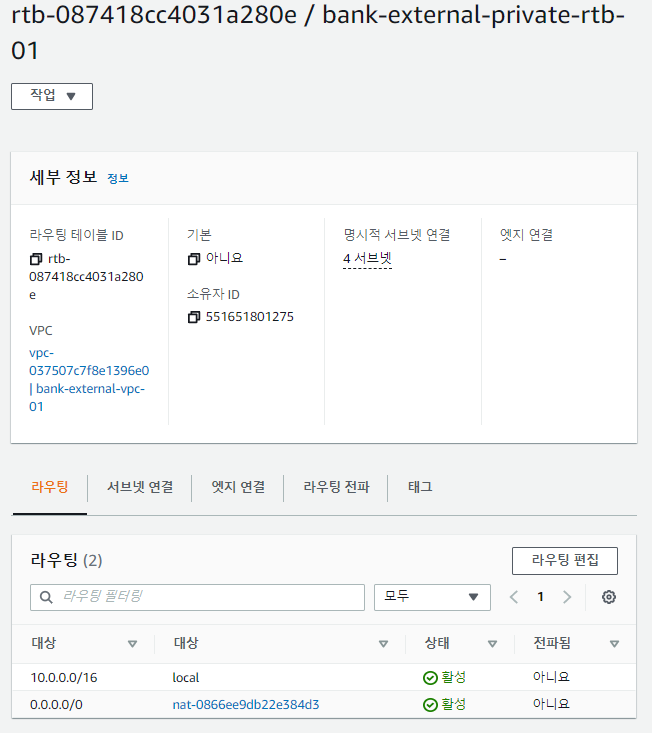
### NAT 게이트웨이

|  |  |
| --- | --- |
| **NAT 게이트웨이 이름** | 서브넷 이름 |
| bank-external-nat-01 | bank-external-edge-subnet-01 |



### 라우팅 테이블

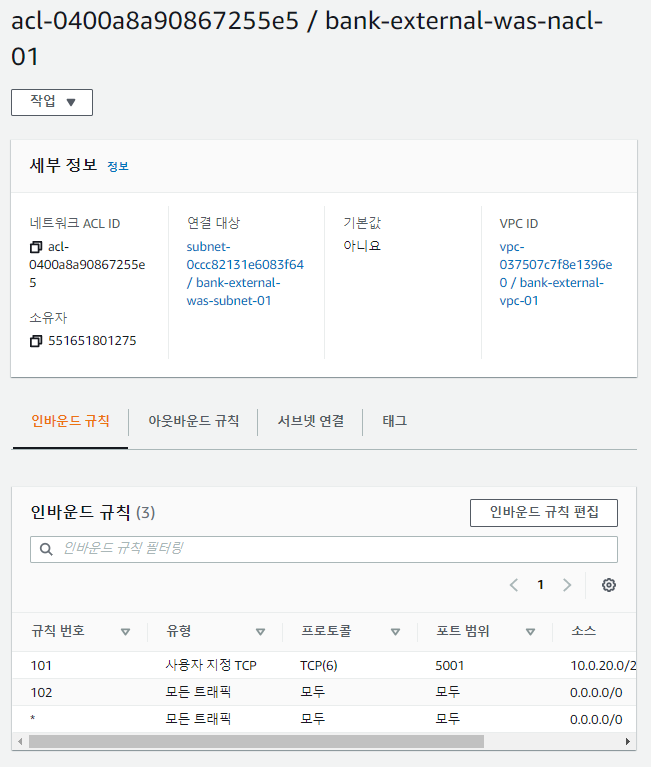
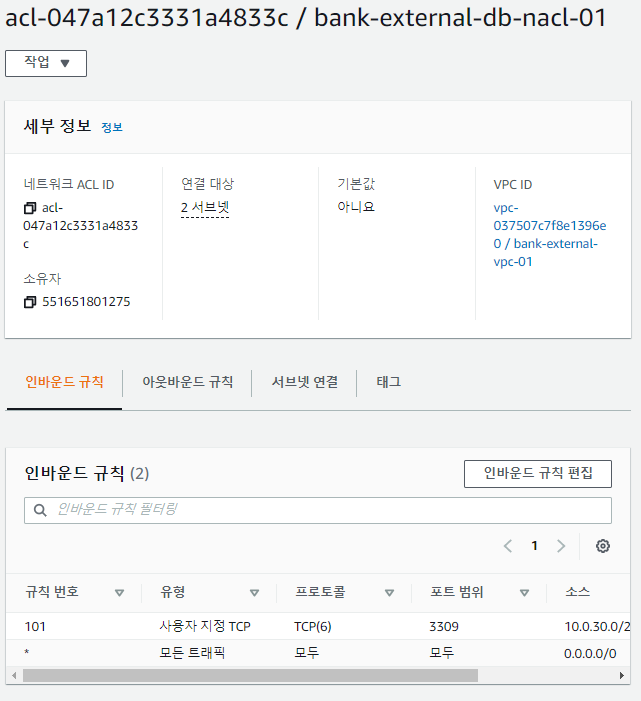
|  |  |  |  |
| --- | --- | --- | --- |
| **라우팅 테이블 이름** | **라우팅: 대상 - 대상** | **명시적 서브넷 연결: 서브넷 이름 - IPv4 CIDR** | **VPC 이름** |
| bank-external-public-rtb-01 | 10.0.0.0/16 - local 0.0.0.0/0 - bank-external-igw-01 | bank-external-edge-subnet-01 - 10.0.0.0/24 bank-external-edge-subnet-02 - 10.0.10.0/24 | bank-external-vpc-01 |
| bank-external-private-rtb-01 | 10.0.0.0/16 - bank-external-nat-01 | bank-external-web-subnet-01 - 10.0.20.0/24 bank-external-was-subnet-01 - 10.0.30.0/24 bank-external-db-subnet-01 - 10.0.40.0/24 bank-external-db-subnet-02 - 10.0.50.0/24 | bank-external-vpc-02 |

### 네트워크 ACL

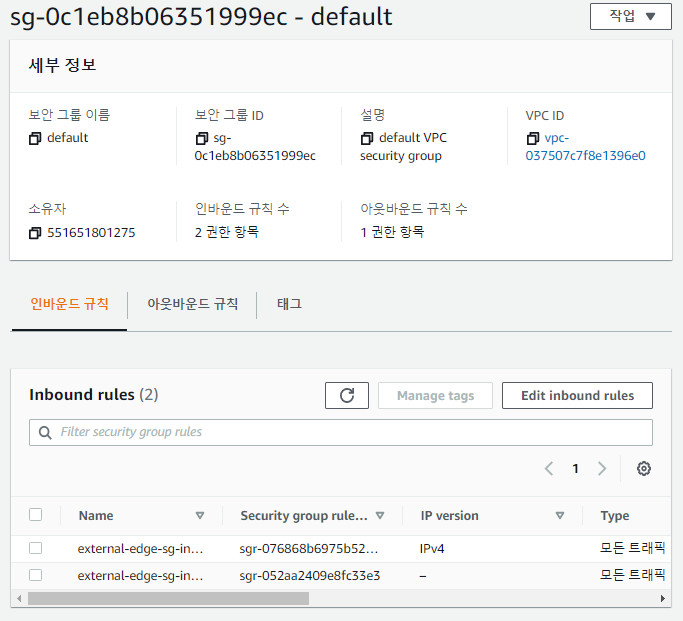
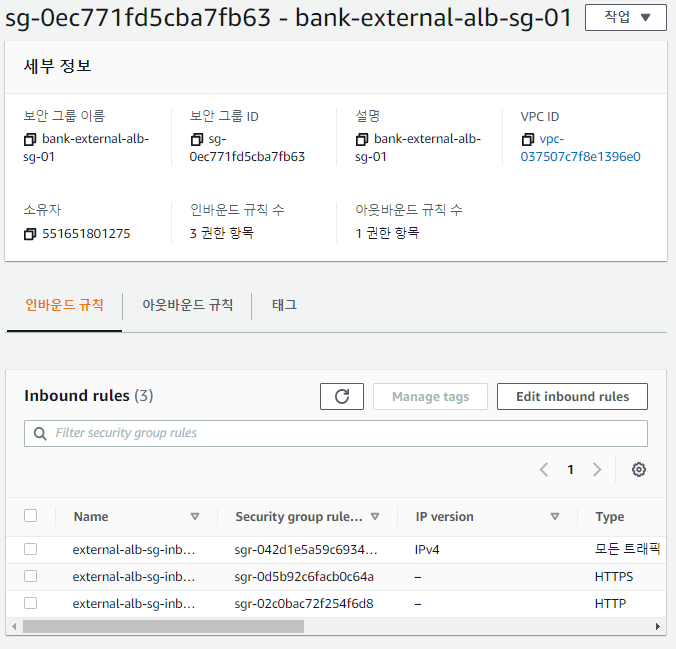
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **네트워크 ACL 이름** | **인바운드 규칙: 규칙번호: 유형(프로토콜, 포트 범위), 소스 [설명]** | **아웃바운드 규칙: 규칙번호: 유형(프로토콜, 포트 범위), 대상 [설명]** | **서브넷 연결** | **VPC 이름** |
| bank-external-edge-nacl-01(기본값) | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 100: 모든 트래픽(모두, 모두), 0.0.0.0/0 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 100: 모든 트래픽(모두, 모두), 0.0.0.0/0 | bank-external-edge-subnet-01 bank-external-edge-subnet-02 | bank-external-vpc-01 |
| bank-external-web-nacl-01 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: HTTP(TCP, 80), 10.0.0.0/24 [웹 접속 - 웹 서버] 102: HTTPS(TCP, 443), 10.0.0.0/24 [웹 접속 - 웹 서버] 103: 모든 트래픽(모두, 모두), 10.0.0.0/16 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: HTTP(TCP, 80), 10.0.0.0/24 [웹 접속 - 웹 서버] 102: HTTPS(TCP, 443), 10.0.0.0/24 [웹 접속 - 웹 서버] 103: 모든 트래픽(모두, 모두), 10.0.0.0/16 | bank-external-web-subnet-01 | bank-external-vpc-01 |
| bank-external-was-nacl-01 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: 사용자 지정 TCP(TCP, 5001), 10.0.20.0/24 [웹 - WAS 통신용] 102: 모든 트래픽(모두, 모두), 10.0.0.0/16 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: 사용자 지정 TCP(TCP, 5001), 10.0.20.0/24 [웹 - WAS 통신용] 102: 모든 트래픽(모두, 모두), 10.0.0.0/16 | bank-external-was-subnet-01 | bank-external-vpc-01 |
| bank-external-db-nacl-01 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: 사용자 지정 TCP(TCP, 3309), 10.0.30.0/24 [My SQL 접속] 102: 모든 트래픽(모두, 모두), 10.0.0.0/16 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: 사용자 지정 TCP(TCP, 3309), 10.0.30.0/24 [My SQL 접속] 102: 모든 트래픽(모두, 모두), 10.0.0.0/16 | bank-external-db-subnet-01 bank-external-db-subnet-02 | bank-external-vpc-01 |

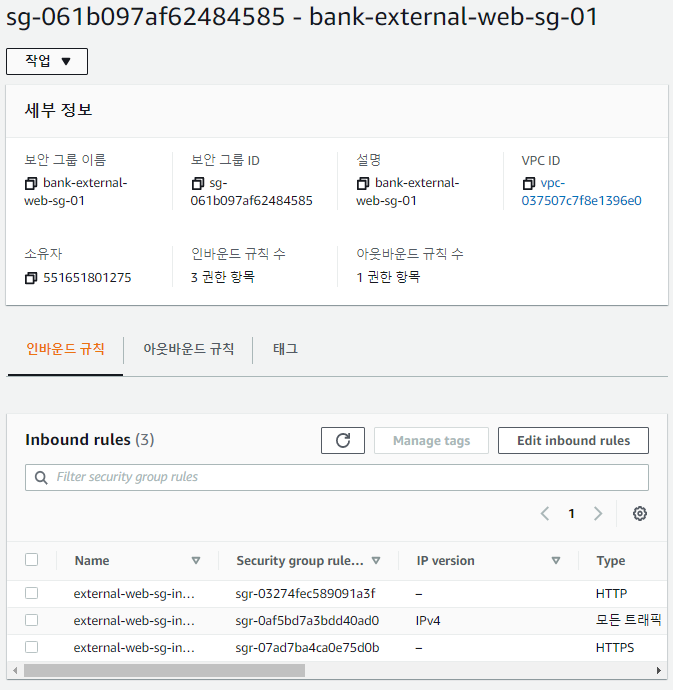
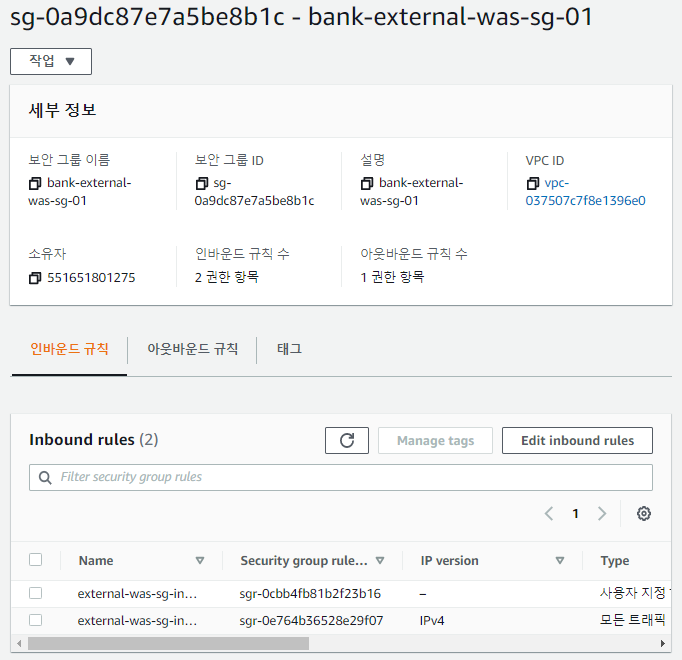
 

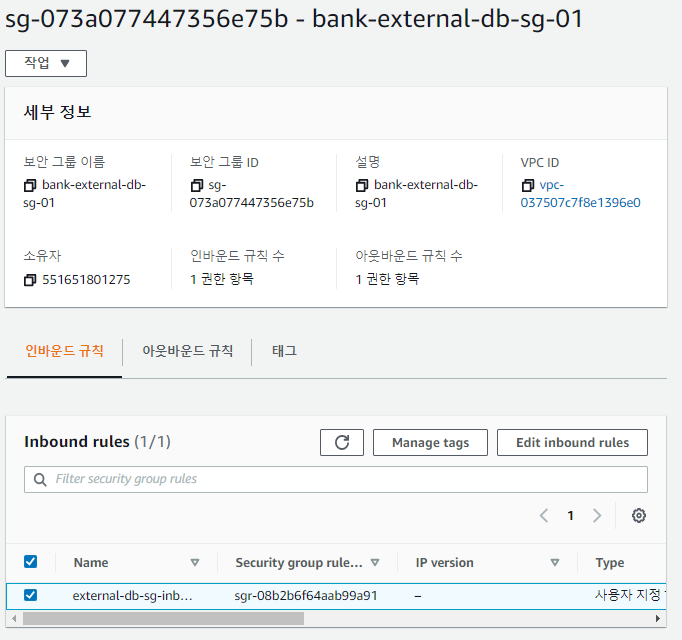
 

### 보안 그룹

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 그룹 이름** | **인바운드 규칙: 인바운드 이름: 유형(프로토콜, 포트 범위), IP 버전(소스) [설명]** | **아웃바운드 규칙: 아웃바운드 이름: 유형(프로토콜, 포트범위), IP 버전(대상) [설명]** | **VPC 이름** |
| bank-external-edge-sg-01(default) | external-edge-sg-inbound-01: 모든 트래픽(전체, 전체), -(sg-0c1eb8b06351999ec / default) external-edge-sg-inbound-02: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | external-edge-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-external-vpc-01 |
| bank-external-alb-sg-01 | external-alb-sg-inbound-01: HTTP(TCP, 80), -(bank-external-edge-sg-01) external-alb-sg-inbound-02: HTTPS(TCP, 443), -(bank-external-edge-sg-01) external-alb-sg-inbound-03: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | external-alb-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-external-vpc-01 |
| bank-external-web-sg-01 | external-web-sg-inbound-01: HTTP(TCP, 80), -(bank-external-alb-sg-01) external-web-sg-inbound-02: HTTPS(TCP, 443), -(bank-external-alb-sg-01) external-web-sg-inbound-03: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | external-web-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-external-vpc-01 |
| bank-external-was-sg-01 | external-was-sg-inbound-01: 사용자 지정 TCP(TCP, 5001), -(bank-external-web-sg-01) external-was-sg-inbound-02: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | external-was-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-external-vpc-01 |
| bank-external-db-sg-01 | external-db-sg-inbound-01: 사용자 지정 TCP(TCP, 3309), -(bank-external-was-sg-01) | external-db-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-external-vpc-01 |

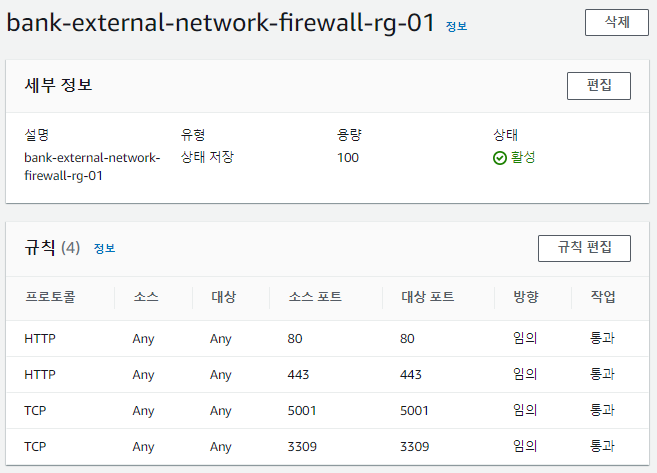
 



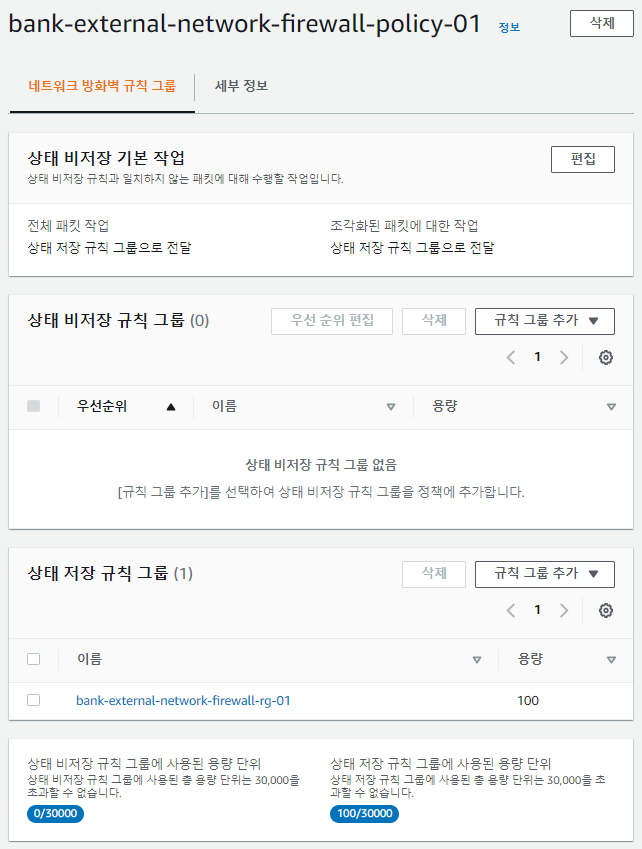
### 네트워크 방화벽 규칙 그룹

|  |  |  |
| --- | --- | --- |
| **네트워크 방화벽 규칙 그룹 이름** | **유형** | **규칙: 프로토콜 - 소스(소스 포트) - 대상(대상 포트) - 방향 - 작업** |
| bank-external-network-firewall-rg-01 | 상태 저장 | HTTP - Any(80) - Any(80) - 임의 - 통과 HTTP - Any(443) - Any(443) - 임의 - 통과 TCP - Any(5001) - Any(5001) - 임의 - 통과 TCP - Any(3309) - Any(3309) - 임의 - 통과 |



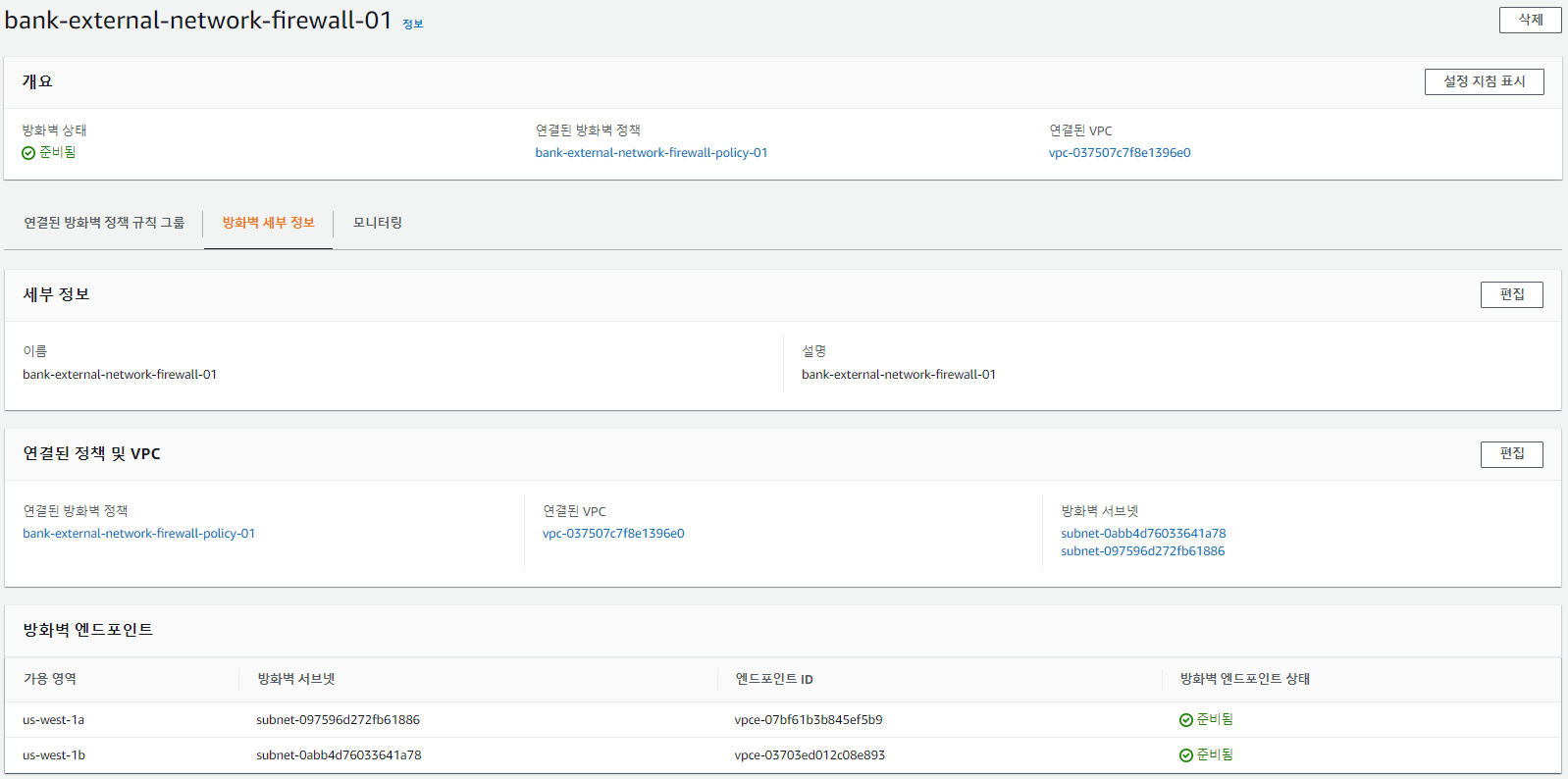
### 네트워크 방화벽 정책

|  |  |
| --- | --- |
| **네트워크 방화벽 정책 이름** | **상태 저장 규칙 그룹** |
| bank-external-network-firewall-policy-01 | bank-external-network-firewall-rg-01 |



### 네트워크 방화벽

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **네트워크 방화벽 이름** | **방화벽 정책** | **가용영역** | **서브넷** | **VPC** |
| bank-external-network-firewall-01 | bank-external-network-firewall-policy-01 | us-west-1a us-west-1b | bank-external-edge-subnet-01 bank-external-edge-subnet-02 | bank-external-vpc-01 |



## bank-external-edge- subntet-01

### 키페어

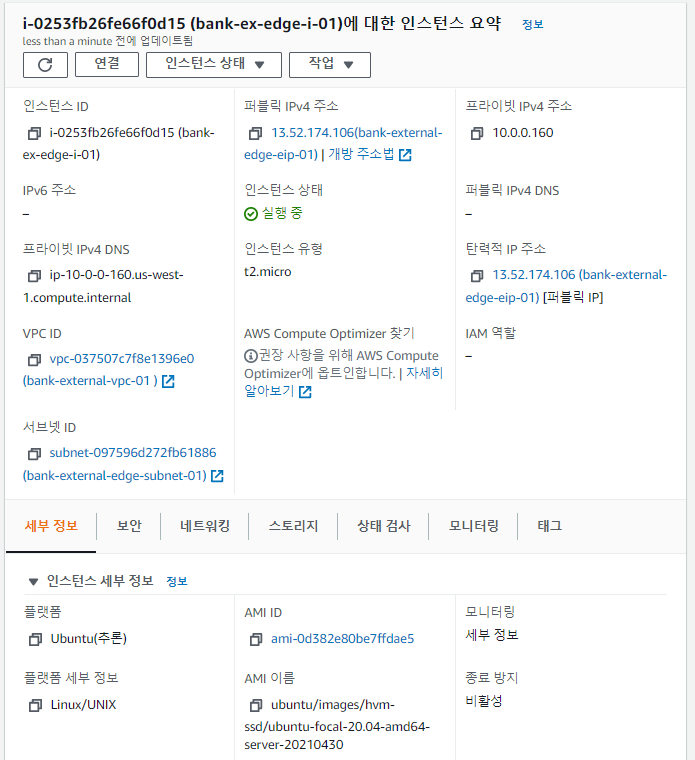
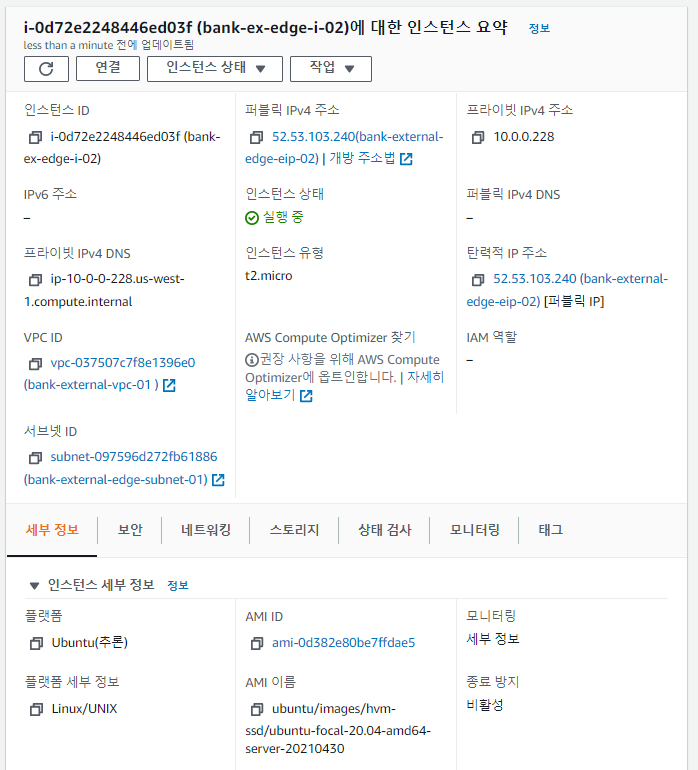
|  |  |
| --- | --- |
| **키 페어 이름** | **유형** |
| bank-ex-edge-key-01 | RSA(.ppk) |



### 인스턴스

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **탄력적 IP 주소 이름** | **인스턴스 이름** | **키 페어 이름** | **보안 그룹 이름** | **서브넷 이름** |
| bank-external-edge-eip-01 | bank-ex-edge-i-01 | bank-ex-edge-key-01 | bank-external-edge-sg-01(default) | bank-external-edge-subnet-01 |
| bank-external-edge-eip-02 | bank-ex-edge-i-02 | bank-ex-edge-key-01 | bank-external-edge-sg-01(default) | bank-external-edge-subnet-01 |

Ubuntu Server 20.04 / 64비트 / 8GB

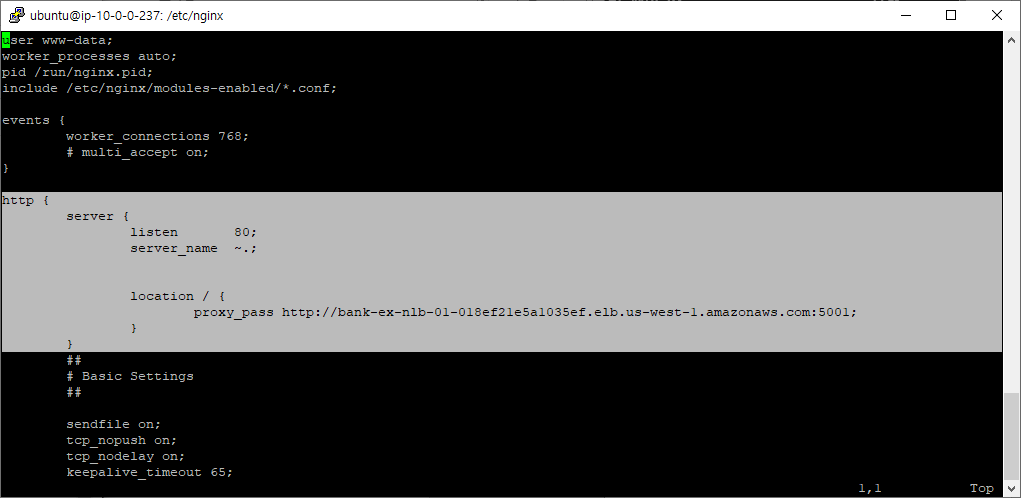
## bank-external-web- subntet-01

### AMI

|  |
| --- |
| **AMI 이름** |
| bank-ex-web-ami-01 |



##### 외부(고객용) Web - /etc/nginx/nginx.conf



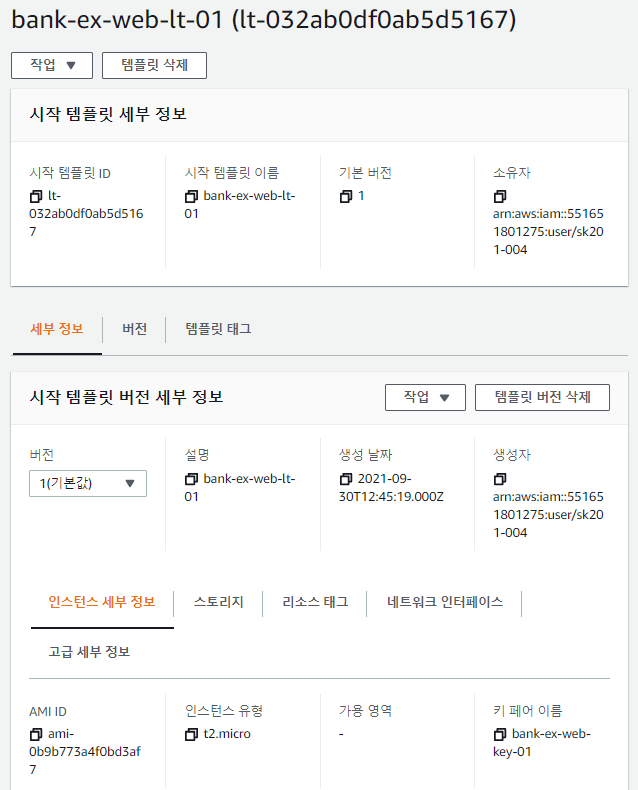
### 키페어

|  |  |
| --- | --- |
| **키 페어 이름** | **유형** |
| bank-ex-web-key-01 | RSA(.ppk) |



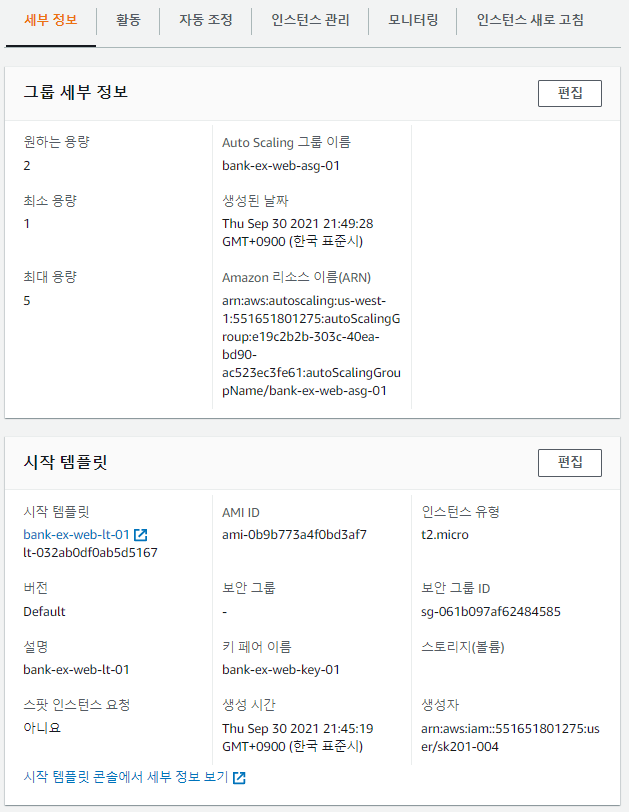
### 시작 템플릿

|  |  |  |
| --- | --- | --- |
| **시작 템플릿 이름** | **키 페어 이름** | **보안 그룹 이름** |
| bank-ex-web-lt-01 | bank-ex-web-key-01 | bank-external-web-sg-01 |



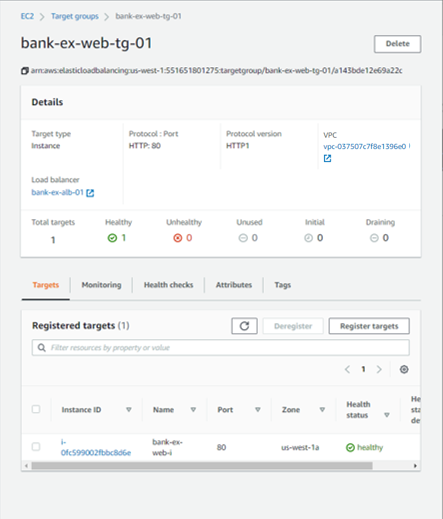
### Auto Scaling 그룹

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Auto Scaling 그룹 이름** | **시작템플릿/구성** | **원하는 용량** | **최소** | **최대** | **로드밸런서 대상 그룹** | **가용 영역** | **서브넷 이름** |
| bank-ex-web-asg-01 | bank-ex-web-lt-01 | 2 | 1 | 5 | bank-ex-web-tg-01 | us-west-1a | bank-external-web-subnet-01 |



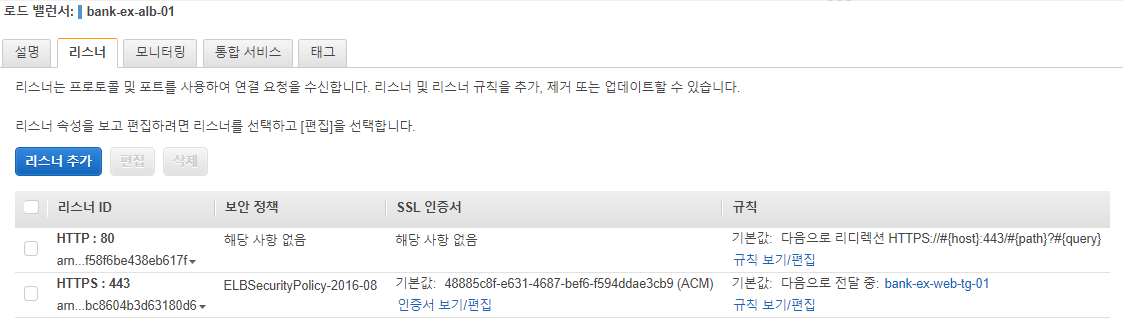
### 대상 그룹

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **대상 그룹 이름** | **Target** | **Target type** | **Protocol : Port** | **Load balancer** | **VPC** |
| bank-ex-web-tg-01 | bank-ex-web-i | Instance | HTTP : 80 | bank-ex-alb-01 | bank-external-vpc-01 |



### 로드밸런서

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **로드밸런서 이름** | **유형** | **체계** | **리스너 Protocol : Port - 대상** | **보안 그룹 이름** | **가용 영역** | **서브넷 이름** | **VPC** 이름 |
| bank-ex-alb-01 | application | internet-facing | HTTP : 80 - 443 리디렉트 HTTPS : 443 - bank-ex-web-tg-01 | bank-external-alb-sg-01 | us-west-1a us-west-1b | bank-external-edge-subnet-01 bank-external-edge-subnet-02 | bank-external-vpc-01 |



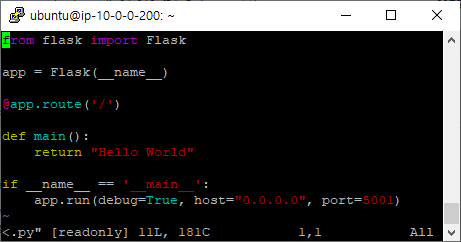
## bank-external-was- subntet-01

### AMI

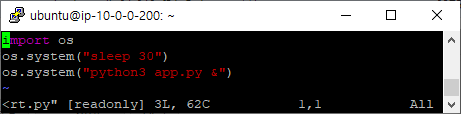
|  |
| --- |
| **AMI 이름** |
| bank-ex-was-ami-01 |



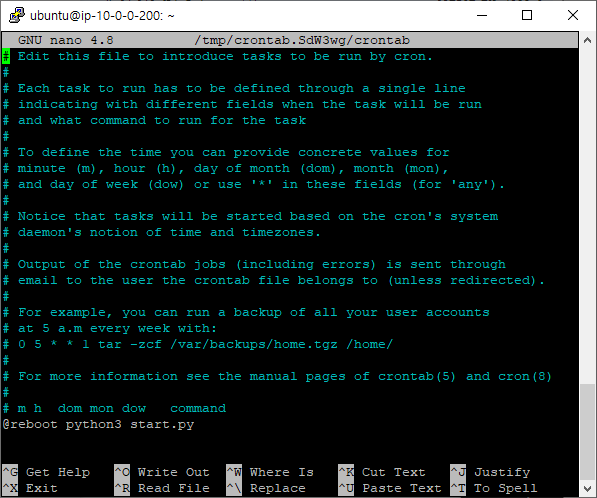
##### 외부(고객용) WAS - app.py



##### 외부(고객용) WAS - start.py



##### 외부(고객용) WAS – crontab -e



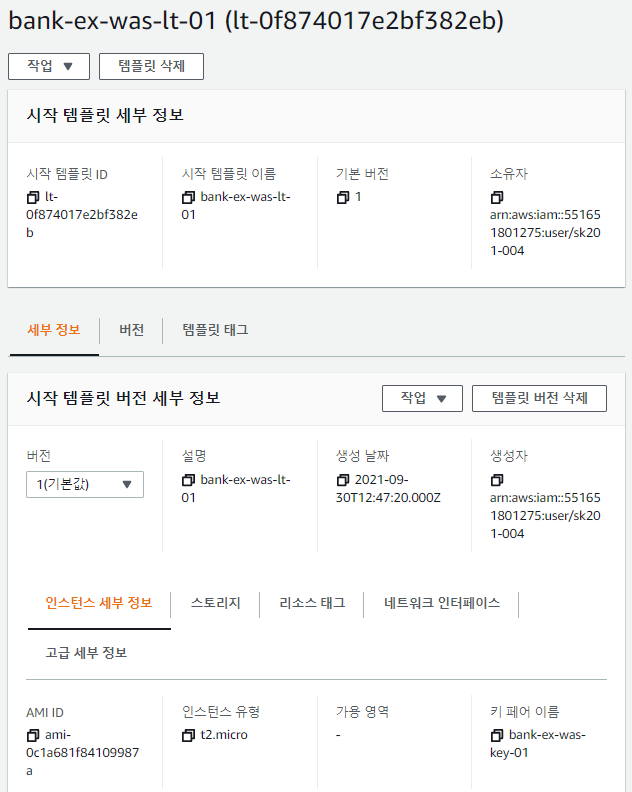
### 키페어

|  |  |
| --- | --- |
| **키 페어 이름** | **유형** |
| bank-ex-was-key-01 | RSA(.ppk) |



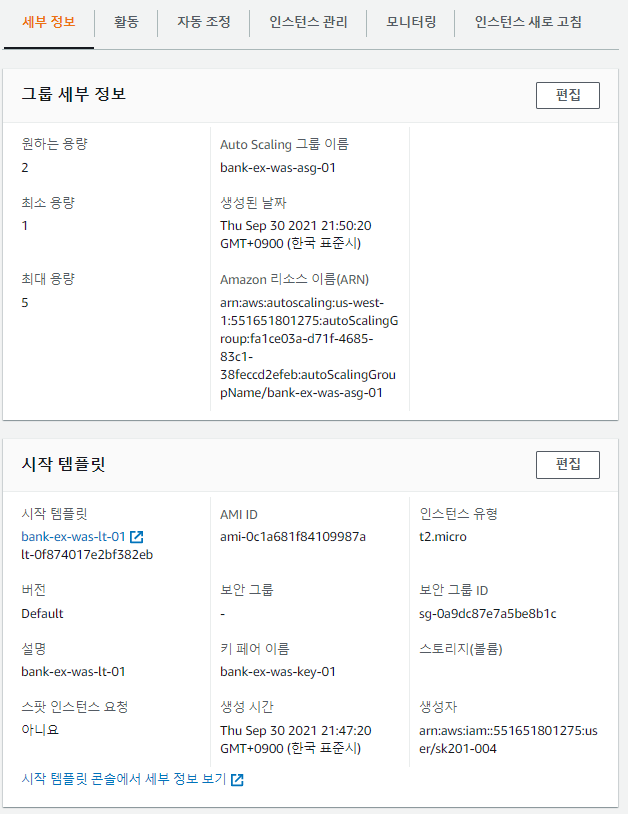
### 시작 템플릿

|  |  |  |
| --- | --- | --- |
| **시작 템플릿 이름** | **키 페어 이름** | **보안 그룹 이름** |
| bank-ex-was-lt-01 | bank-ex-was-key-01 | bank-external-was-sg-01 |



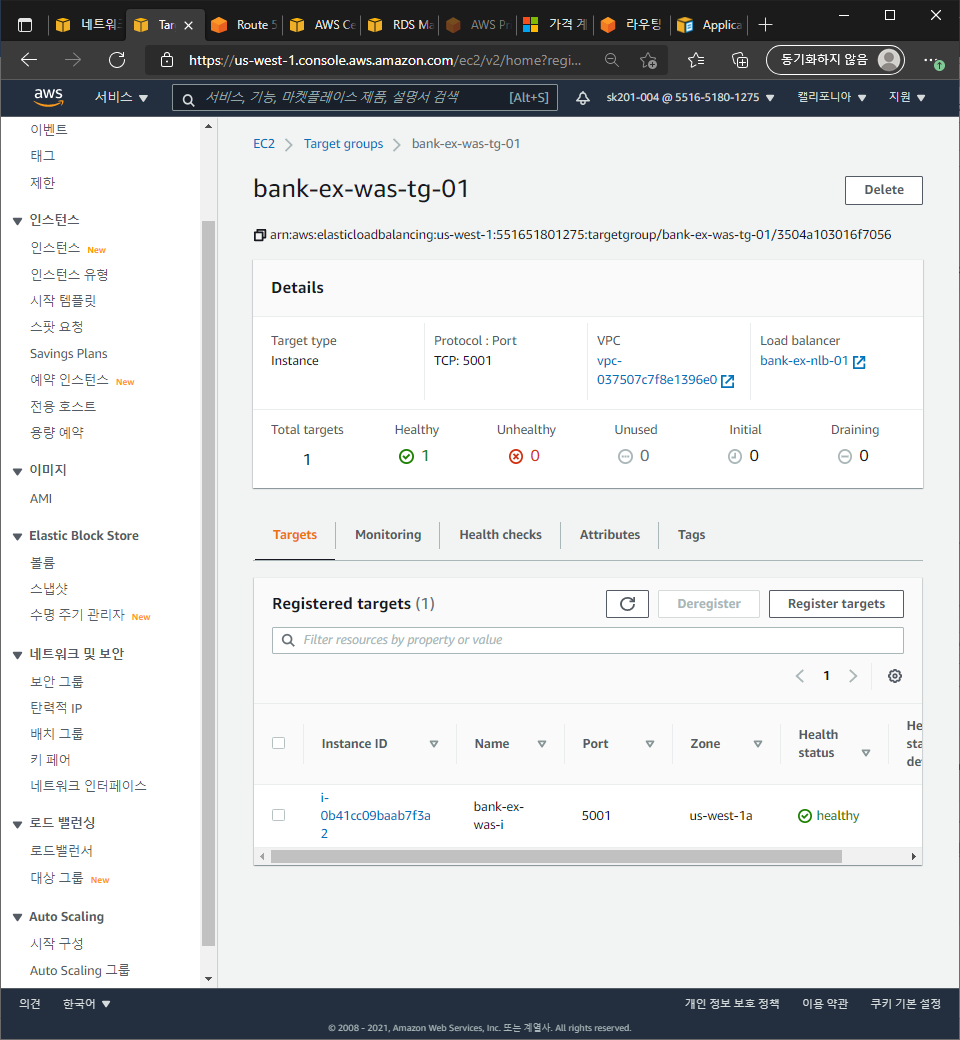
### Auto Scaling 그룹

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Auto Scaling 그룹 이름** | **시작템플릿/구성** | **원하는 용량** | **최소** | **최대** | **로드밸런서 대상그룹** | **가용 영역** | **서브넷 이름** |
| bank-ex-was-asg-01 | bank-ex-was-lt-01 | 2 | 1 | 5 | bank-ex-was-tg-01 | us-west-1a | bank-external-was-subnet-01 |



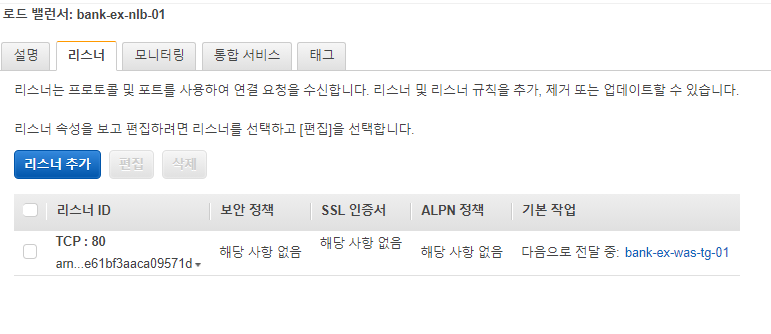
### 대상 그룹

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **대상 그룹 이름** | **Target** | **Target type** | **Protocol : Port** | **Load balancer** | **VPC** |
| bank-ex-was-tg-01 | bank-ex-was-i | Instance | TCP : 5001 | bank-ex-nlb-01 | bank-external-vpc-01 |



### 로드밸런서

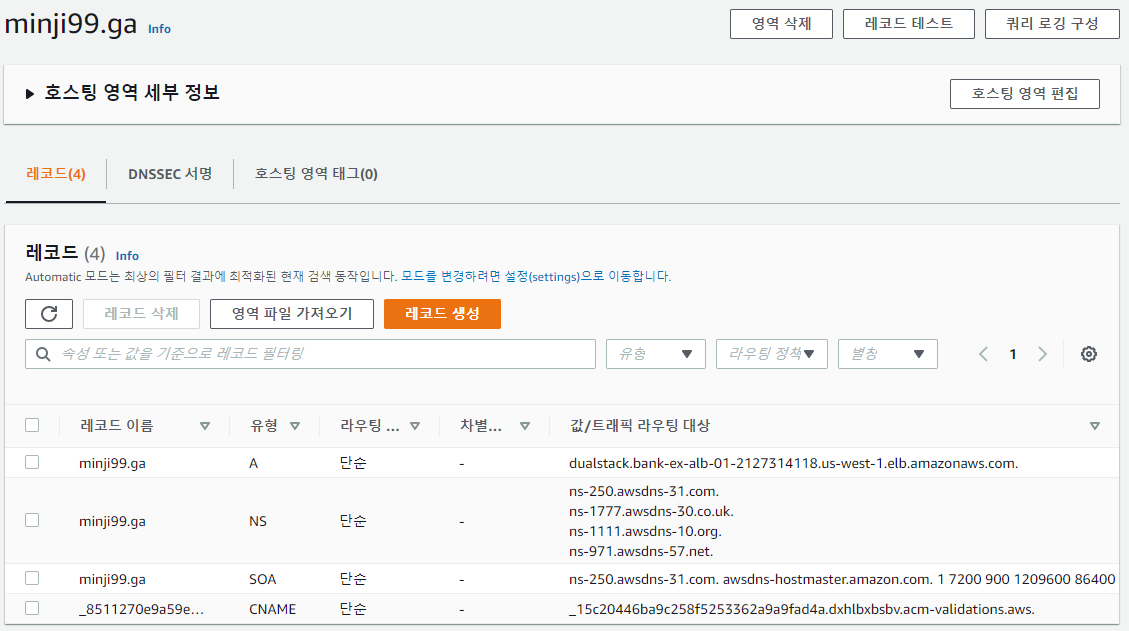
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **로드밸런서 이름** | **유형** | **체계** | **리스너 Protocol : Port - 대상** | **가용 영역** | **서브넷 이름** | **VPC** 이름 |
| bank-ex-nlb-01 | network | internal | TCP : 5001 | us-west-1a | bank-external-was-subnet-01 | bank-external-vpc-01 |



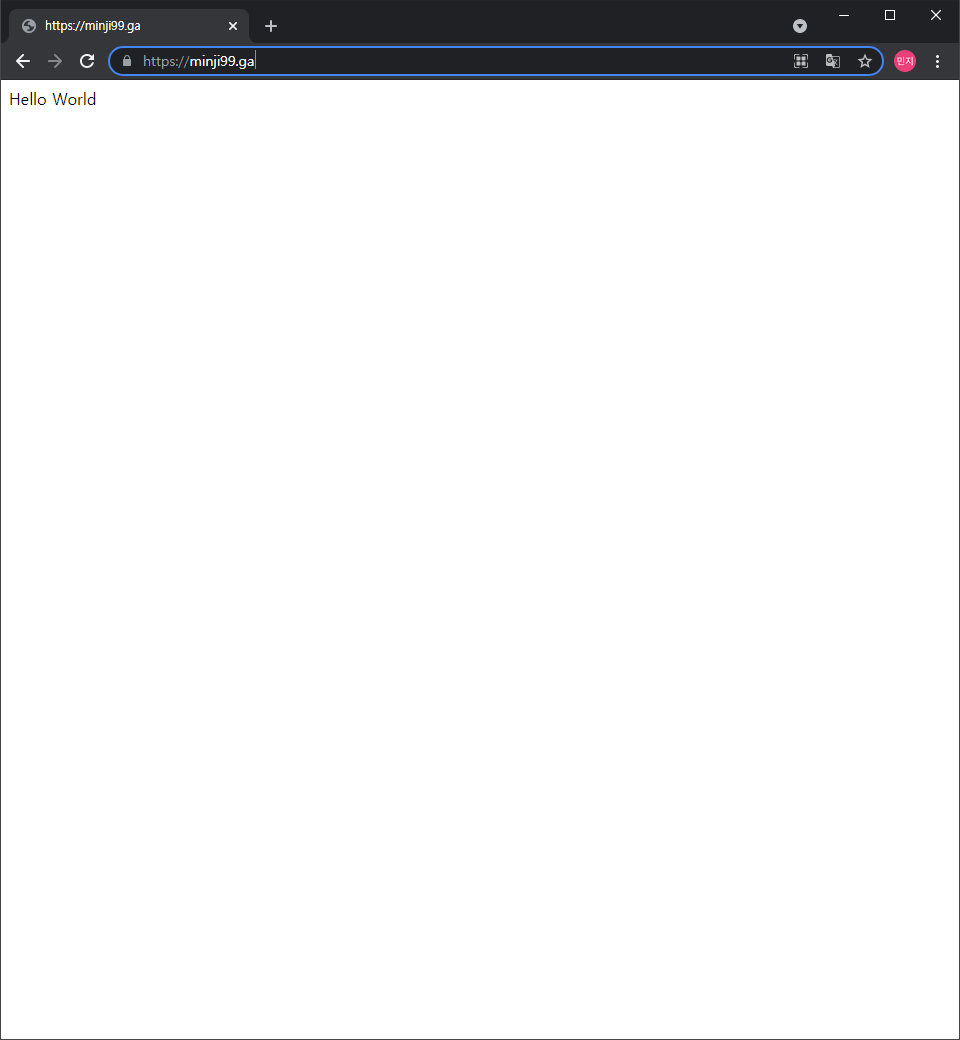
## Route53

### 호스팅 영역

|  |  |  |
| --- | --- | --- |
| **도메인 이름** | **유형** | **레코드: 레코드 이름 - 유형 - 값/트래픽 라우팅 대상** |
| minji99.ga | 퍼블릭 | minji99.ga - NS - ns-81.awsdns-10.com. minji99.ga - NS - ns-1858.awsdns-40.co.uk. minji99.ga - NS - ns-882.awsdns-46.net. minji99.ga - NS - ns-1448.awsdns-53.org.  minji99.ga - SOA - ns-81.awsdns-10.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400  \_8511270e9a59e2f4a299f5bb8c9cd7fe.minji99.ga - CNAME - \_15c20446ba9c258f5253362a9a9fad4a.dxhlbxbsbv.acm-validations.aws.  minji99.ga - A - dualstack.bank-ex-alb-01-2127314118.us-west-1.elb.amazonaws.com. |



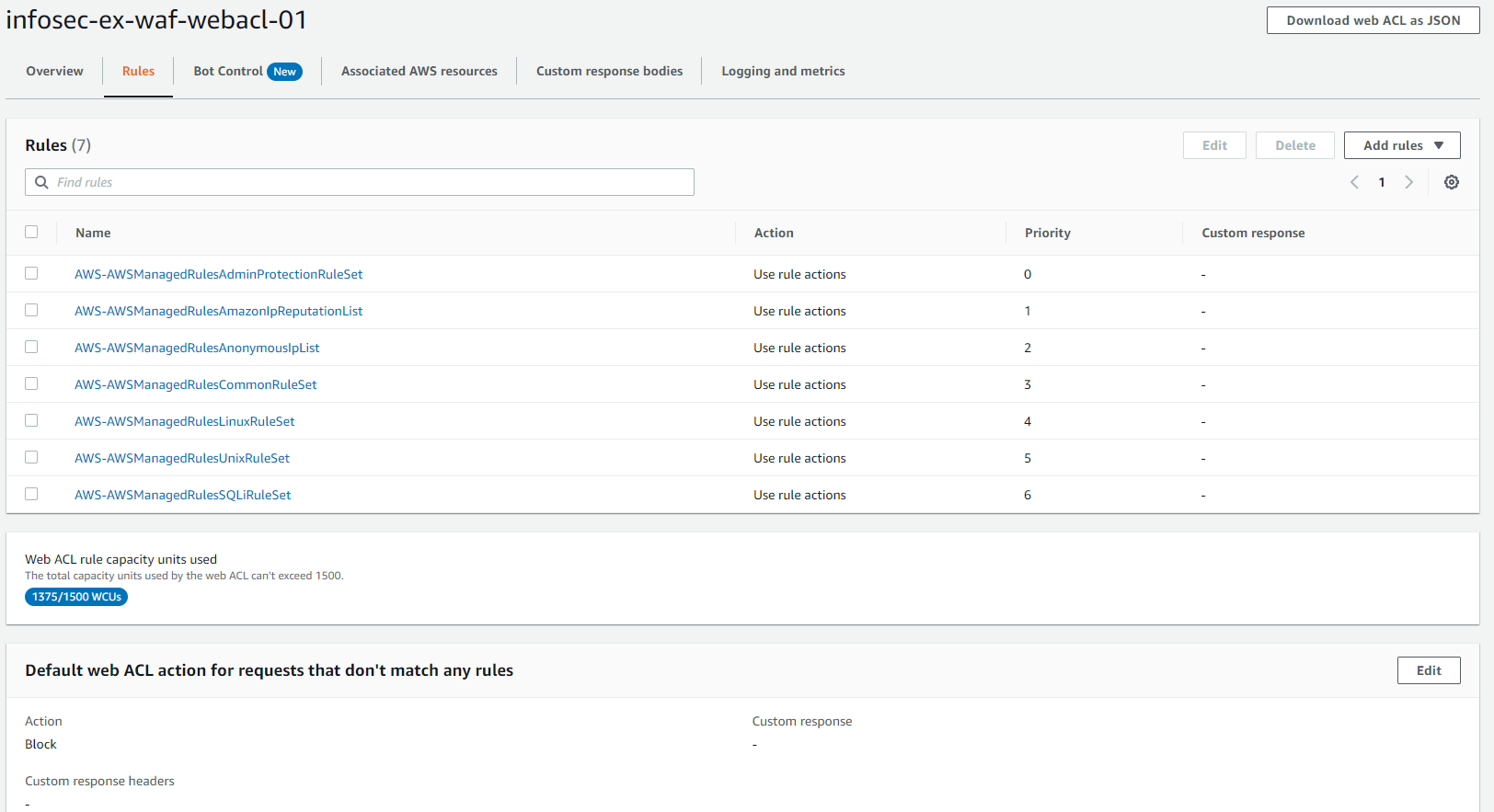
##### 외부(고객용) Web 및 WAS 연동



## WAF & Shield

### Web ACLs

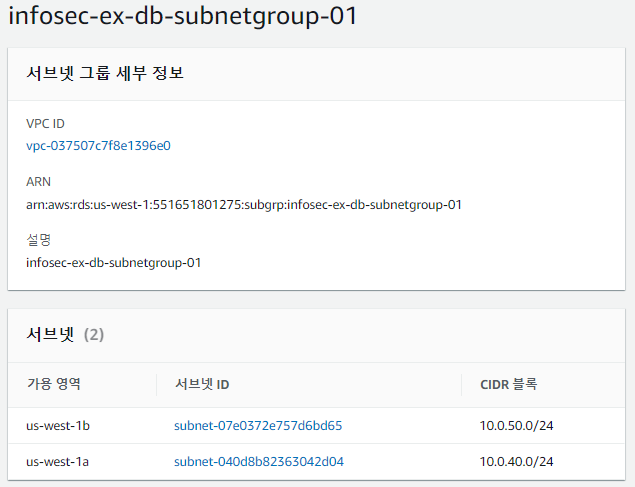
|  |  |  |  |
| --- | --- | --- | --- |
| **Web ACLs 이름** | **Rules: Priority: Name - Action** | **Default web ACL action for requests that don't match any rules** | **Associated AWS resources: Name - Resource type -Region** |
| infosec-ex-waf-webacl-01 | 0: AWS-AWSManagedRulesAdminProtectionRuleSet - Use rule actions 1: AWS-AWSManagedRulesAmazonIpReputationList - Use rule actions 2: AWS-AWSManagedRulesAnonymousIpList - Use rule actions 3: AWS-AWSManagedRulesCommonRuleSet - Use rule actions 4: AWS-AWSManagedRulesLinuxRuleSet - Use rule actions 5: AWS-AWSManagedRulesUnixRuleSet - Use rule actions 6: AWS-AWSManagedRulesSQLiRuleSet - Use rule actions | Block | bank-ex-alb-01 - Application Load Balancer -US West (N. California) |



## bank-external-db-subntet-01 & bank-external-db-subntet-02

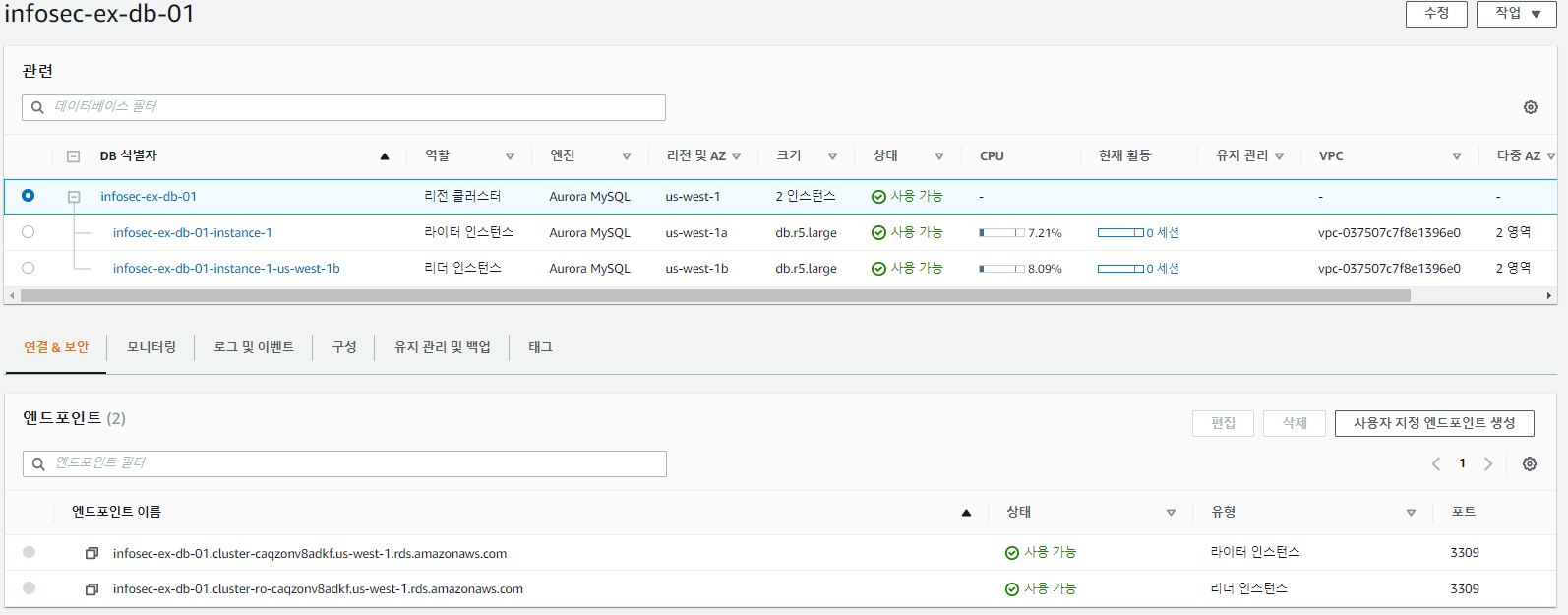
### 서브넷 그룹

|  |  |  |
| --- | --- | --- |
| **서브넷 그룹 이름** | **서브넷 이름** | **IP(CIDR)** |
| infosec-ex-db-subnetgroup-01 | infosec-external-db-subnet-01 infosec-external-db-subnet-02 | 10.0.40.0/24 10.0.50.0/24 |



### 데이터베이스

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **DB 이름** | **역할** | **포트** | **가용 영역** | **보안 그룹 이름** | **서브넷 그룹 이름** | **VPC 이름** |
| infosec-ex-db-01 | 리전 클러스터 |  | us-west-1 |  |  |  |
| infosec-ex-db-01-instance-1 | 라이터 인스턴스 | 3309 | us-west-1a | infosec-external-db-sg-01 | infosec-ex-ex-db-subnetgroup-01 | infosec-external-vpc-01 |
| infosec-ex-db-01-instance-1-us-west-1b | 리더 인스턴스 | 3309 | us-west-1b | infosec-external-db-sg-01 | infosec-ex-ex-db-subnetgroup-01 | infosec-external-vpc-01 |

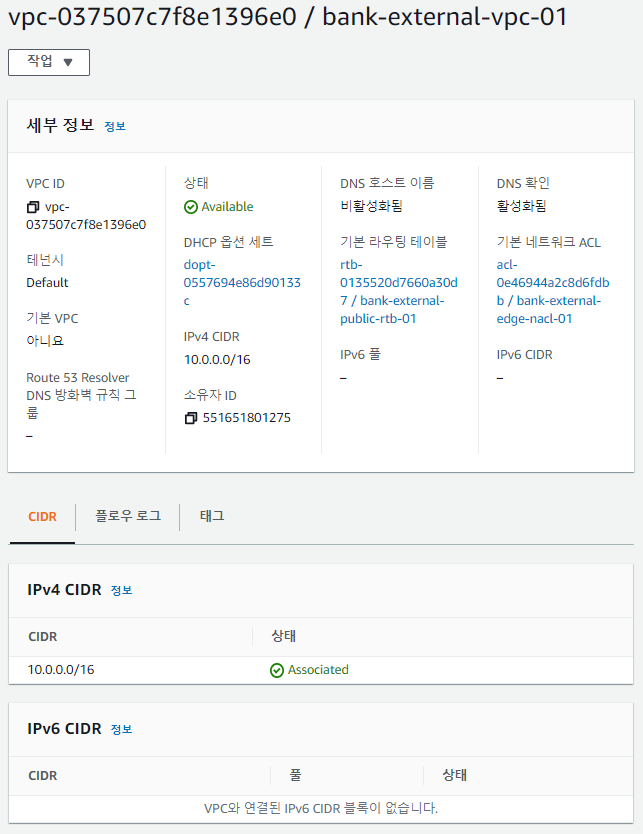


# 내부(직원용) 인프라 구성

## VPC

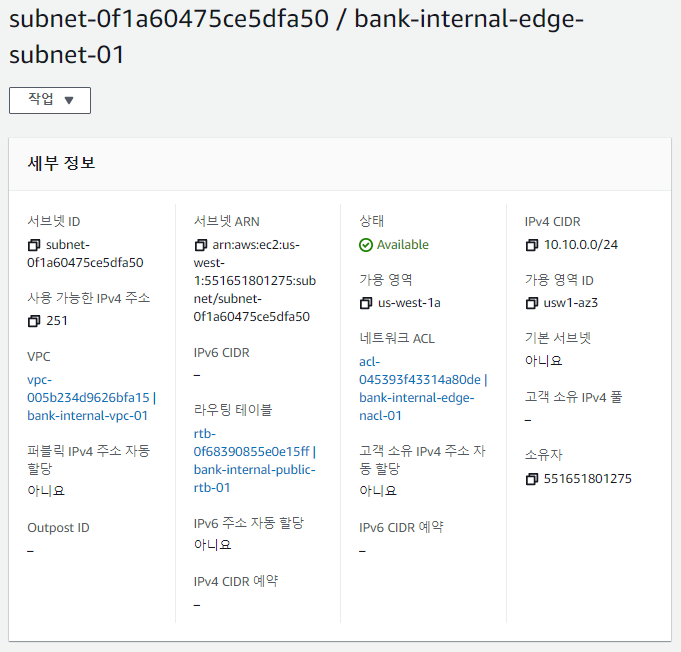
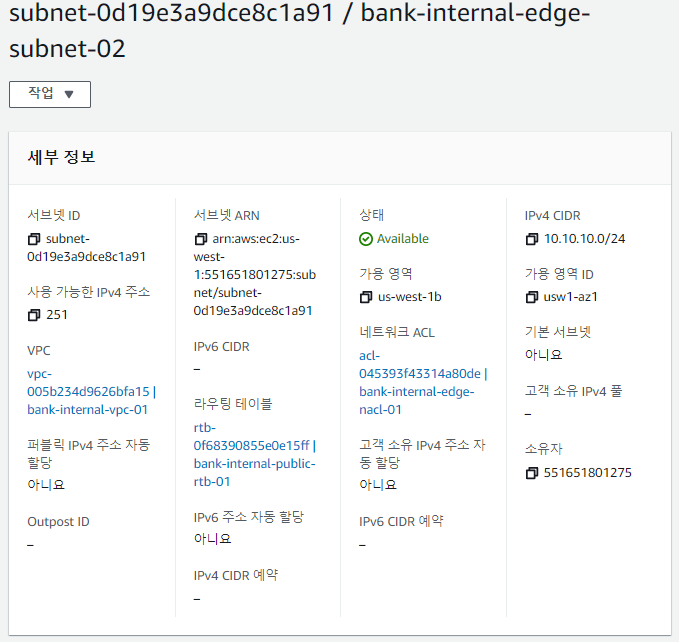
### VPC

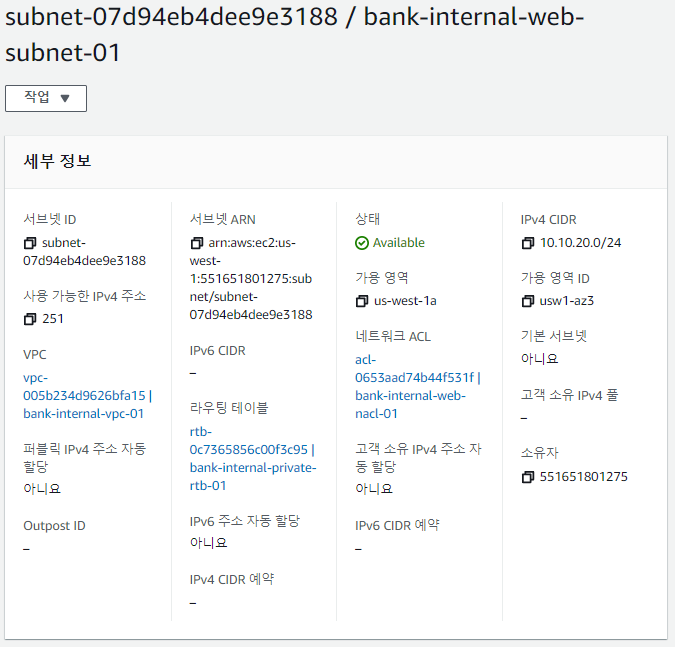
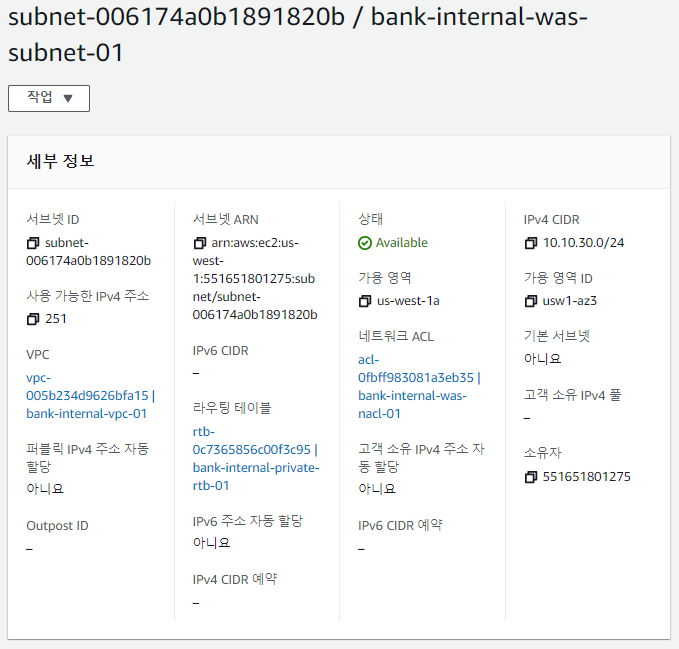
|  |  |
| --- | --- |
| **IP(CIDR)** | **VPC 이름** |
| 10.10.0.0/16 | bank-internal-vpc-01 |

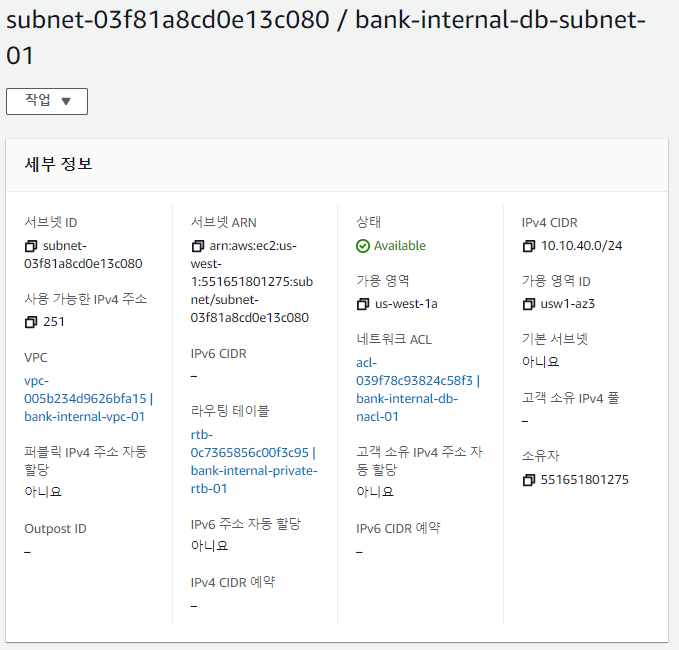
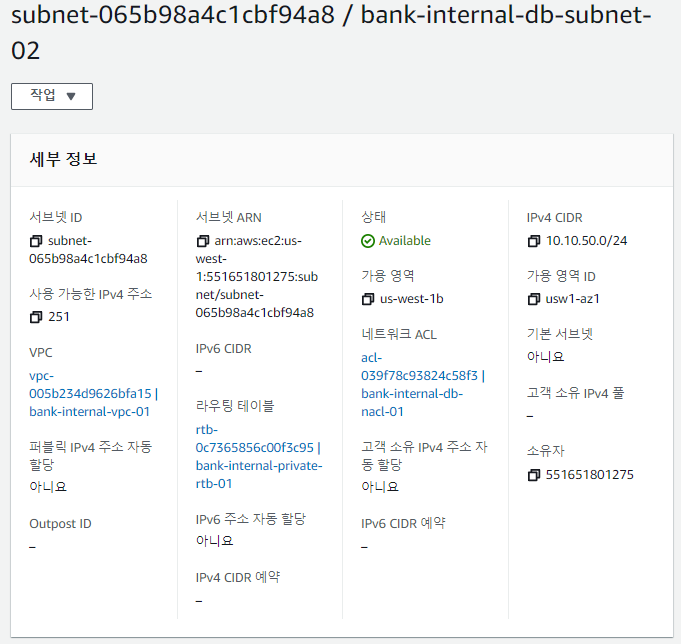


### 서브넷

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP(CIDR)** | **서브넷 이름** | **가용영역** | **가용영역 ID** | **VPC 이름** |
| 10.10.0.0/24 | bank-internal-edge-subnet-01 | us-west-1a | usw1-az3 | bank-internal-vpc-01 |
| 10.10.10.0/24 | bank-internal-edge-subnet-02 | us-west-1b | usw1-az1 | bank-internal-vpc-01 |
| 10.10.20.0/24 | bank-internal-web-subnet-01 | us-west-1a | usw1-az3 | bank-internal-vpc-01 |
| 10.10.30.0/24 | bank-internal-was-subnet-01 | us-west-1a | usw1-az3 | bank-internal-vpc-01 |
| 10.10.40.0/24 | bank-internal-db-subnet-01 | us-west-1a | usw1-az3 | bank-internal-vpc-01 |
| 10.10.50.0/24 | bank-internal-db-subnet-02 | us-west-1b | usw1-az1 | bank-internal-vpc-01 |

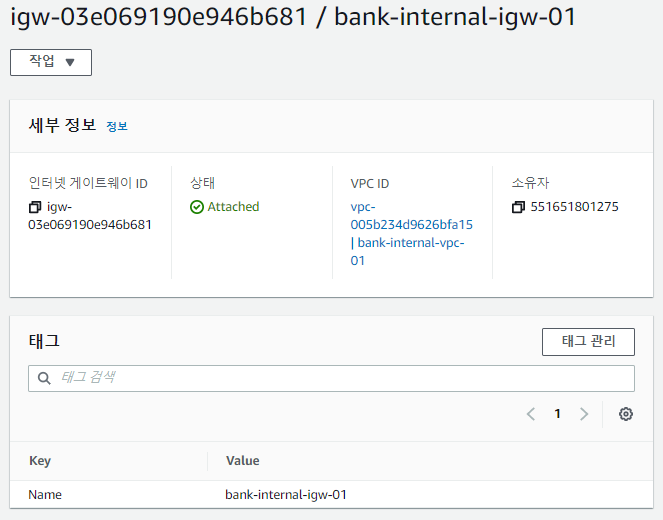
 

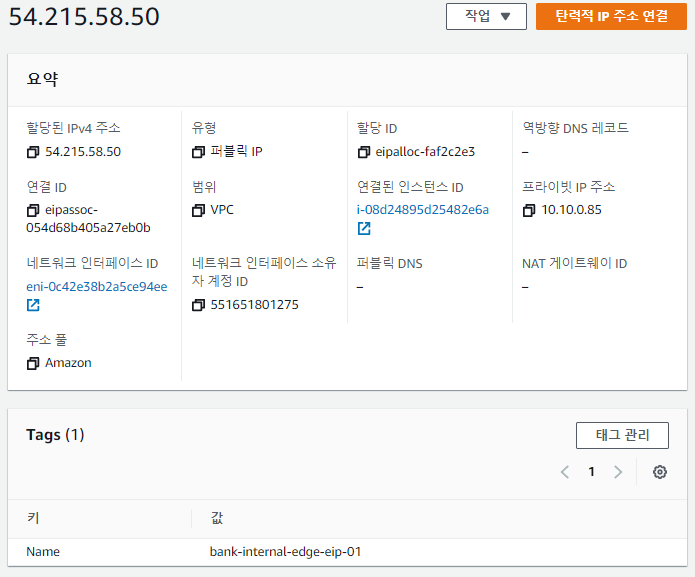
### 인터넷 게이트웨이

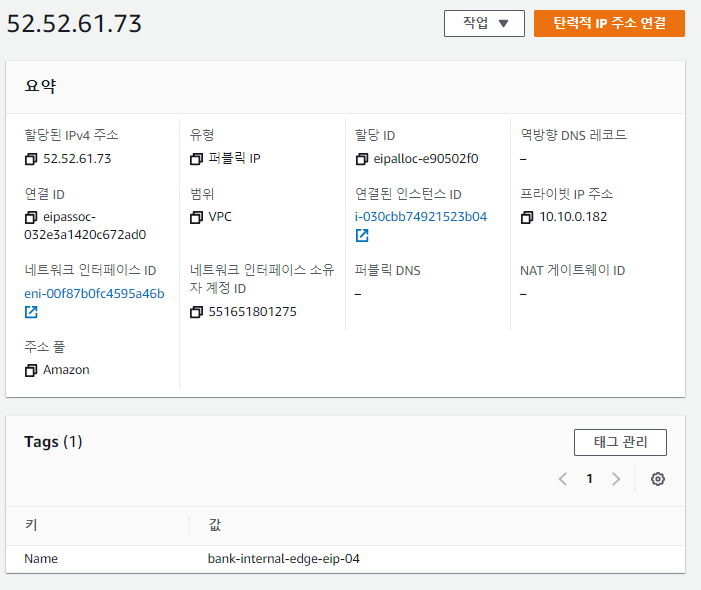
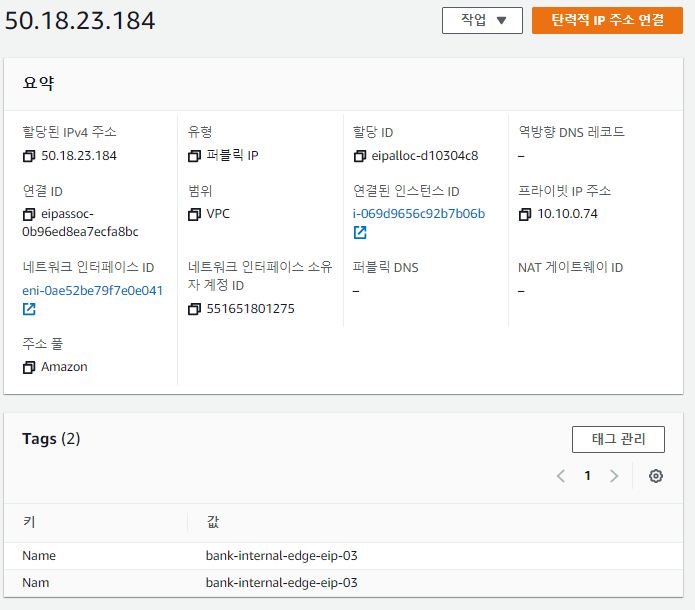
|  |  |
| --- | --- |
| **인터넷 게이트웨이 이름** | **VPC** 이름 |
| bank-internal-igw-01 | bank-internal-vpc-01 |



### 탄력적 IP 주소

|  |
| --- |
| **탄력적 IP 주소 이름** |
| bank-internal-edge-eip-01 |
| bank-internal-edge-eip-02 |
| bank-internal-edge-eip-03 |
| bank-internal-edge-eip-04 |
| bank-internal-nat-eip-01 |

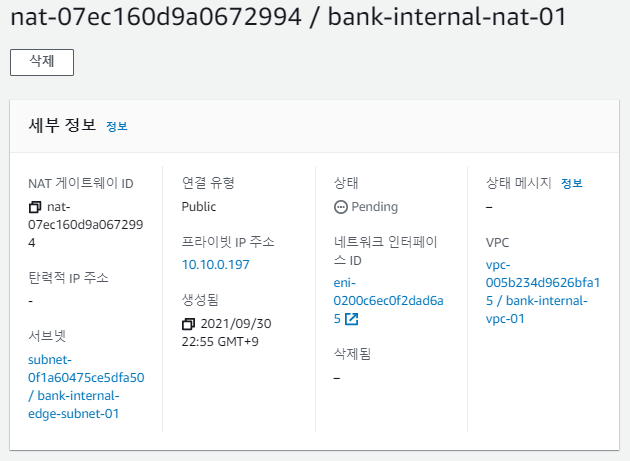






### NAT 게이트웨이

|  |  |
| --- | --- |
| **NAT 게이트웨이 이름** | **서브넷 이름** |
| bank-internal-nat-01 | bank-internal-edge-subnet-01 |



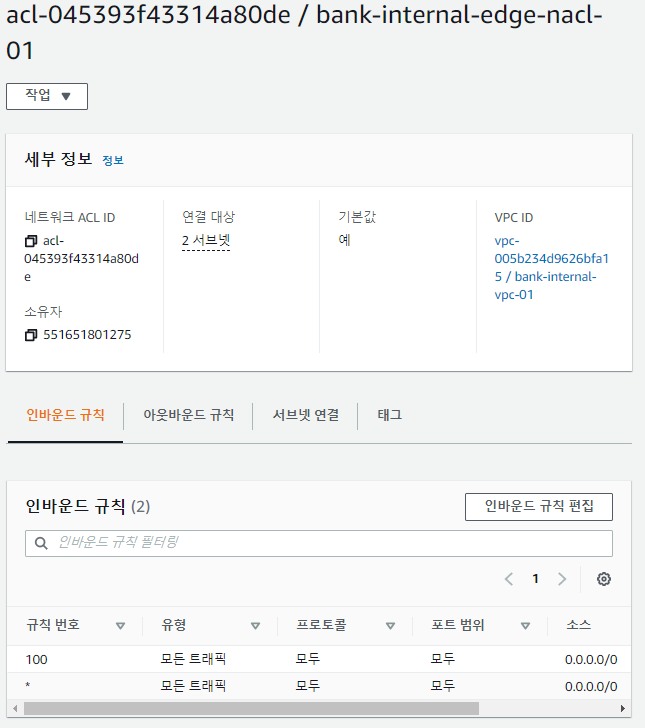
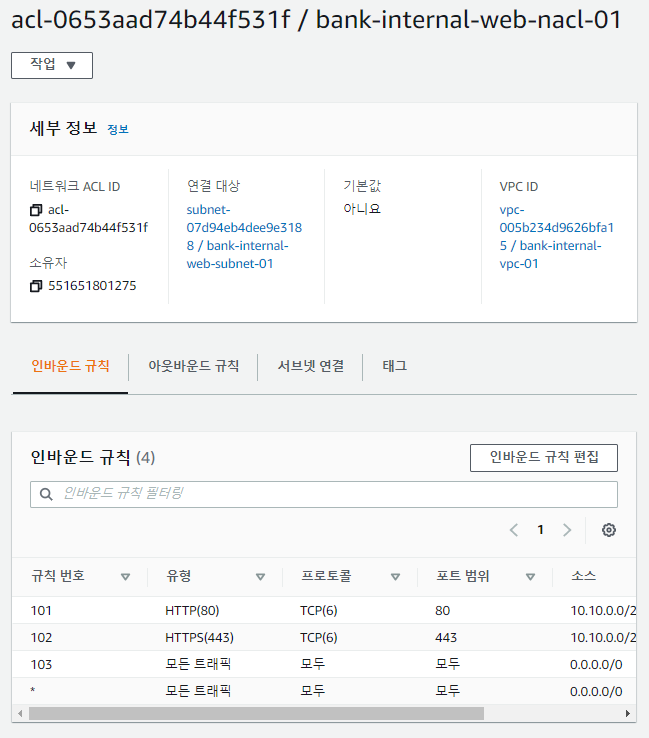
### 라우팅 테이블

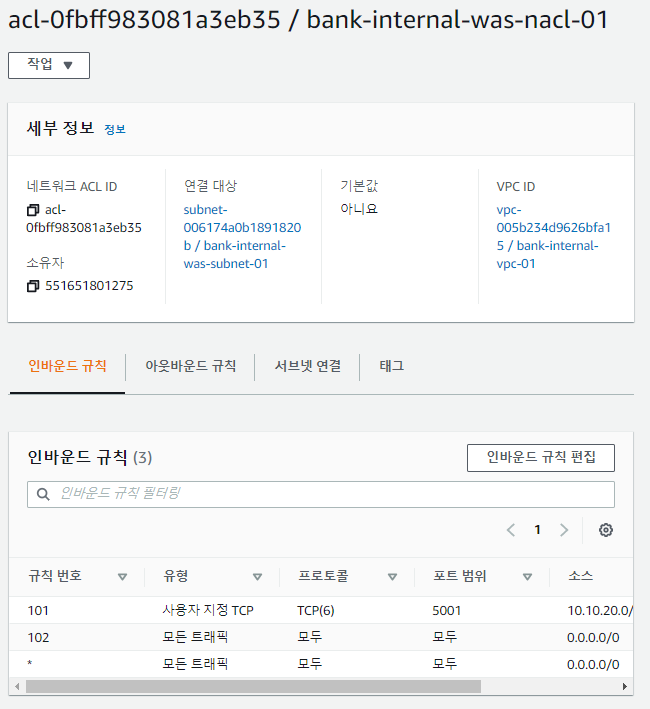
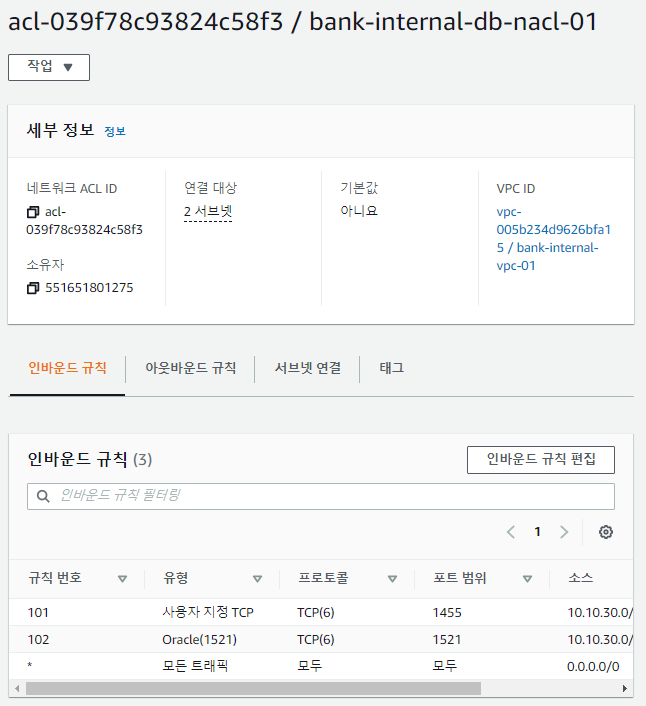
|  |  |  |  |
| --- | --- | --- | --- |
| **라우팅 테이블 이름** | **라우팅: 대상 - 대상** | **명시적 서브넷 연결: 서브넷 이름 - IPv4 CIDR** | **VPC 이름** |
| bank-internal-public-rtb-01 | 10.0.10.0/16 - local 0.0.0.0/0 - bank-internal-igw-01 | subnet-0f1a60475ce5dfa50 / bank-internal-edge-subnet-01 - 10.10.0.0/24 subnet-0d19e3a9dce8c1a91 / bank-internal-edge-subnet-01 - 10.10.10.0/24 | bank-internal-vpc-01 |
| bank-internal-private-rtb-01 | 10.0.0.0/16 - local 0.0.0.0/0 - bank-internal-nat-01 | subnet-07d94eb4dee9e3188 / bank-external-web-subnet-01 - 10.10.20.0/24 subnet-006174a0b1891820b / bank-external-was-subnet-01 - 10.10.30.0/24 subnet-03f81a8cd0e13c080 / bank-external-db-subnet-01 - 101.0.40.0/24 subnet-065b98a4c1cbf94a8 / bank-external-db-subnet-02 - 10.10.50.0/24 | bank-internal-vpc-01 |

### 네트워크 ACL

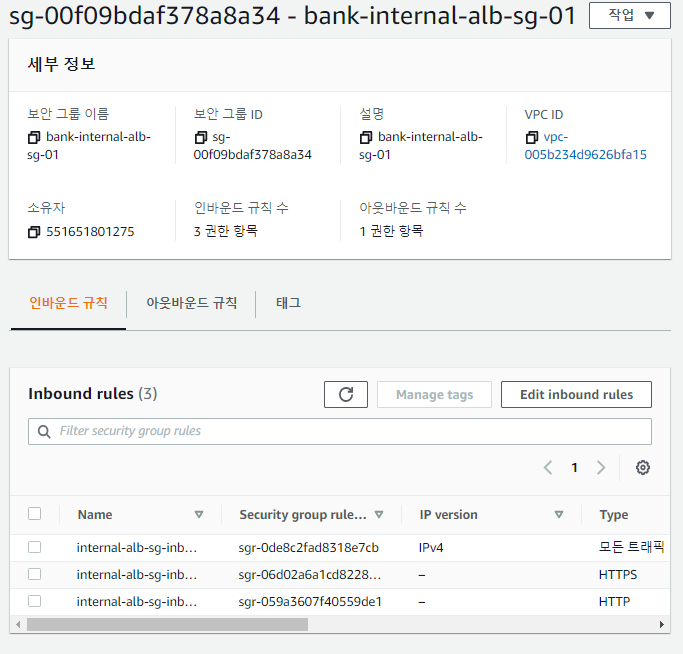
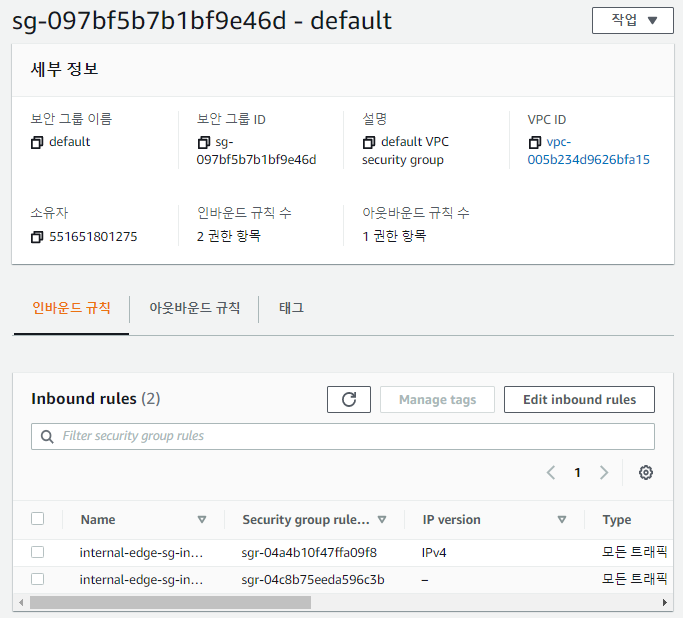
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **네트워크 ACL 이름** | **인바운드 규칙: 규칙번호: 유형(프로토콜, 포트 범위), 소스 [설명]** | **아웃바운드 규칙: 규칙번호: 유형(프로토콜, 포트 범위), 대상 [설명]** | **서브넷 연결** | **VPC 이름** |
| bank-internal-edge-nacl-01(기본값) | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 100: 모든 트래픽(모두,모두), 0.0.0.0/0 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 100: 모든 트래픽(모두, 모두), 0.0.0.0/0 | bank-internal-edge-subnet-01 bank-internal-edge-subnet-02 | bank-internal-vpc-01 |
| bank-internal-web-nacl-01 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: HTTP(TCP, 80), 10.10.0.0/24 [웹 접속 - 웹 서버] 102: HTTPS(TCP, 443), 10.10.0.0/24 [웹 접속 - 웹 서버] 103: 모든 트래픽(모두, 모두), 10.10.0.0/16 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: HTTP(TCP, 80), 10.10.0.0/24 [웹 접속 - 웹 서버] 102: HTTPS(TCP, 443), 10.10.0.0/24 [웹 접속 - 웹 서버] 103: 모든 트래픽(모두, 모두), 10.10.0.0/16 | bank-internal-web-subnet-01 | bank-internal-vpc-01 |
| bank-internal-was-nacl-01 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: 사용자 지정 TCP(TCP, 5001), 10.10.20.0/24 [웹 - WAS 통신용] 102: 모든 트래픽(모두, 모두), 10.10.0.0/16 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0  101: 사용자 지정 TCP(TCP, 5001), 10.10.20.0/24 [웹 - WAS 통신용] 102: 모든 트래픽(모두, 모두), 10.10.0.0/16 | bank-internal-was-subnet-01 | bank-internal-vpc-01 |
| bank-internal-db-nacl-01 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: 사용자 지정 TCP(TCP,1455), 10.10.30.0/24 [MS SQL 접속] 102: Oracle(TCP,1521), 10.10.30.0/24 [Oracle 접속] 103: 모든 트래픽(모두, 모두), 10.10.0.0/16 | \*: 모든 트래픽(모두, 모두), 0.0.0.0/0 101: 사용자 지정 TCP(TCP,1455), 10.10.30.0/24 [MS SQL 접속] 102: Oracle(TCP,1521), 10.10.30.0/24 [Oracle 접속] 103: 모든 트래픽(모두, 모두), 10.10.0.0/16 | bank-internal-db-subnet-01 bank-internal-db-subnet-02 | bank-internal-vpc-01 |

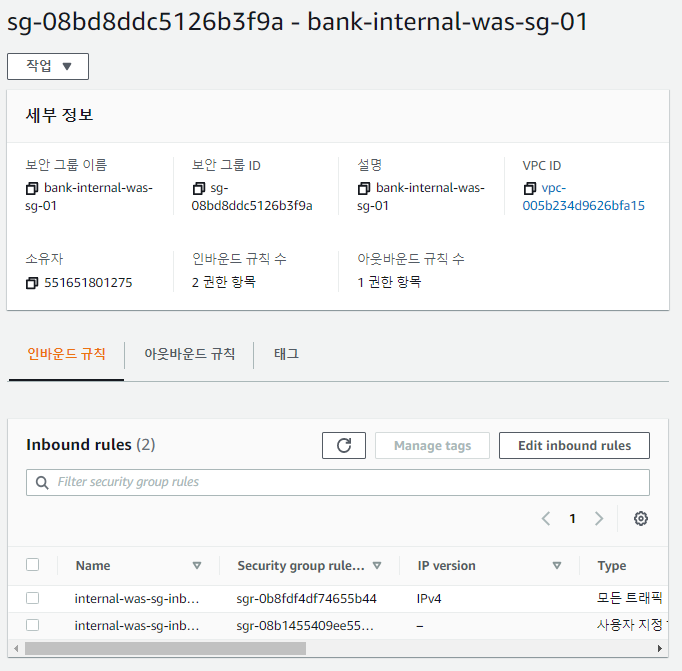
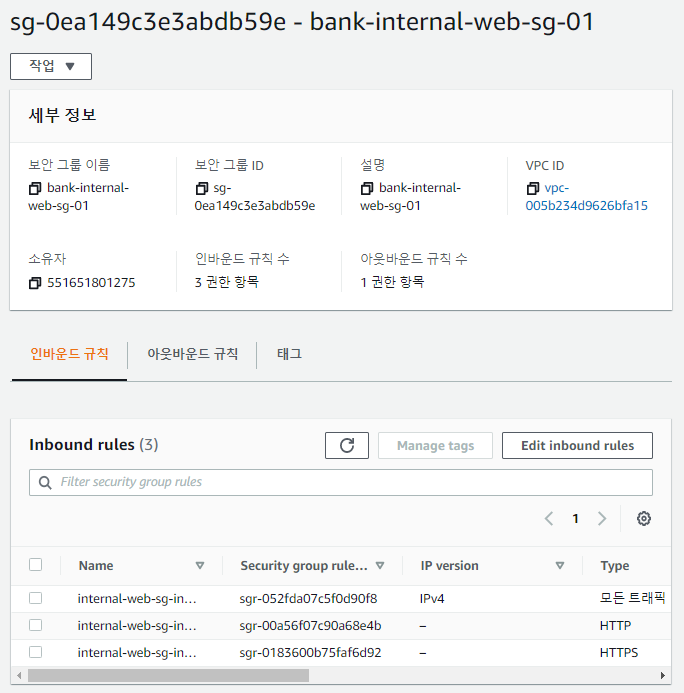
 

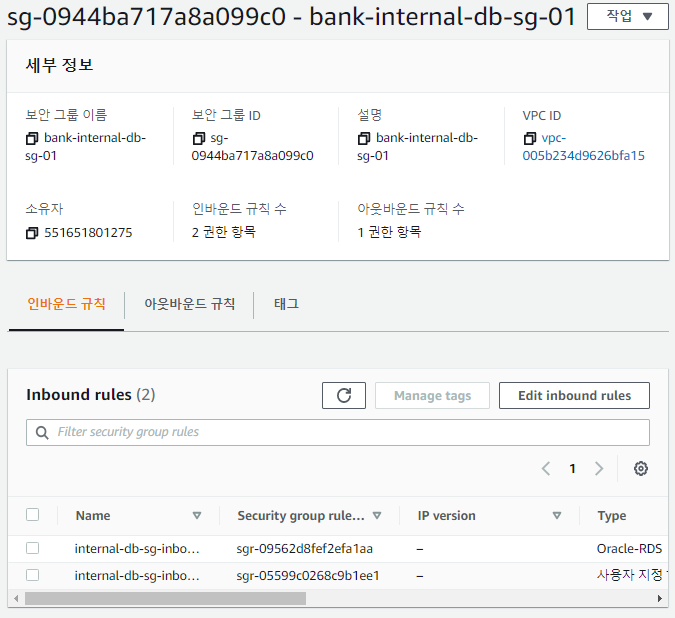
 

### 보안 그룹

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 그룹 이름** | **인바운드 규칙: 인바운드 이름: 유형(프로토콜, 포트 범위), IP 버전(소스) [설명]** | **아웃바운드 규칙: 아웃바운드 이름: 유형(프로토콜, 포트범위), IP 버전(대상) [설명]** | **VPC 이름** |
| bank-internal-edge-sg-01(default) | internal-edge-sg-inbound-01: 모든 트래픽(전체, 전체), -(sg-097bf5b7b1bf9e46d / default) internal-edge-sg-inbound-02: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | infternal-edge-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-internal-vpc-01 |
| bank-internal-alb-sg-01 | internal-alb-sg-inbound-01: HTTP(TCP, 80), -(bank-internal-edge-sg-01) internal-alb-sg-inbound-02: HTTPS(TCP, 443), -(bank-internal-edge-sg-01) internal-alb-sg-inbound-03: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | infternal-alb-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-internal-vpc-01 |
| bank-internal-web-sg-01 | internal-web-sg-inbound-01: HTTP(TCP, 80), -(bank-internal-alb-sg-01) internal-web-sg-inbound-02: HTTPS(TCP, 443), -(bank-internal-alb-sg-01) internal-web-sg-inbound-03: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | infternal-web-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-internal-vpc-01 |
| bank-internal-was-sg-01 | internal-was-sg-inbound-01: 사용자 지정 TCP(TCP, 5001), -(bank-einernal-web-sg-01) internal-was-sg-inbound-02: 모든 트래픽(전체, 전체), -(0.0.0.0/0) | infternal-was-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-internal-vpc-01 |
| bank-internal-db-sg-01 | internal-db-sg-inbound-01: 사용자 지정 TCP(TCP,1455), -(bank-internal-was-sg-01) [MS SQL 접속] internal-db-sg-inbound-02: Oracle(TCP,1521), -(bank-internal-was-sg-01) [Oracle 접속] | infternal-db-sg-outbound-01: 모든 트래픽(전체, 전체), IPv4(0.0.0.0/0) | bank-internal-vpc-01 |

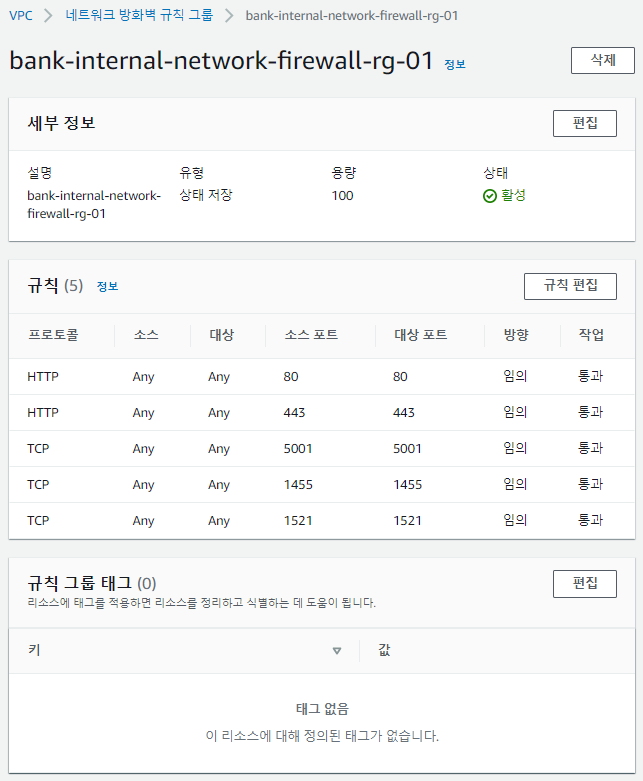






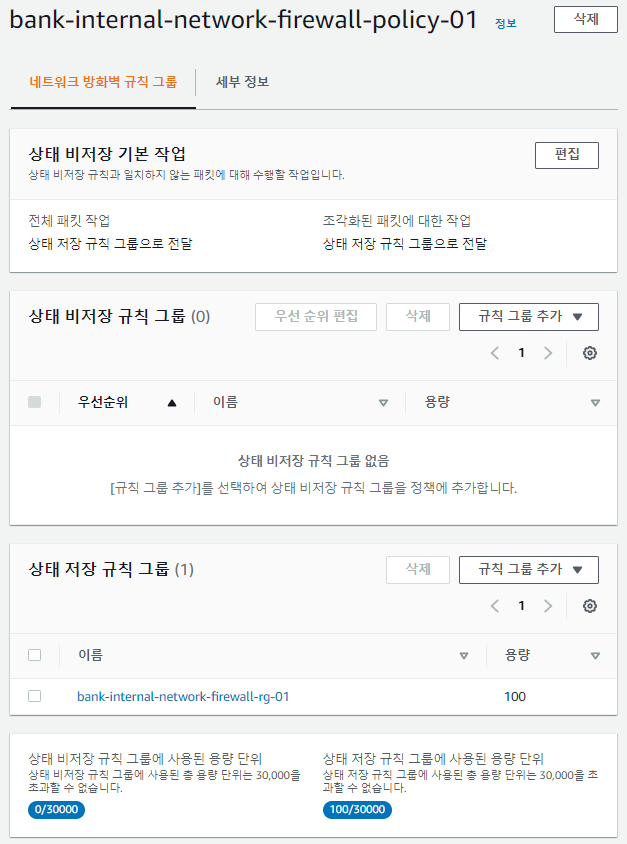
### 네트워크 방화벽 규칙 그룹

|  |  |  |
| --- | --- | --- |
| **네트워크 방화벽 규칙 그룹 이름** | **유형** | **규칙: 프로토콜 - 소스(소스 포트) - 대상(대상 포트) - 방향 - 작업** |
| bank-internal-network-firewall-rg-01 | 상태 저장 | HTTP - Any(80) - Any(80) - 임의 - 통과 HTTP - Any(443) - Any(443) - 임의 - 통과 TCP - Any(5001) - Any(5001) - 임의 - 통과 TCP - Any(1455) - Any(1455) - 임의 - 통과 TCP - Any(1521) - Any(1521) - 임의 - 통과 |



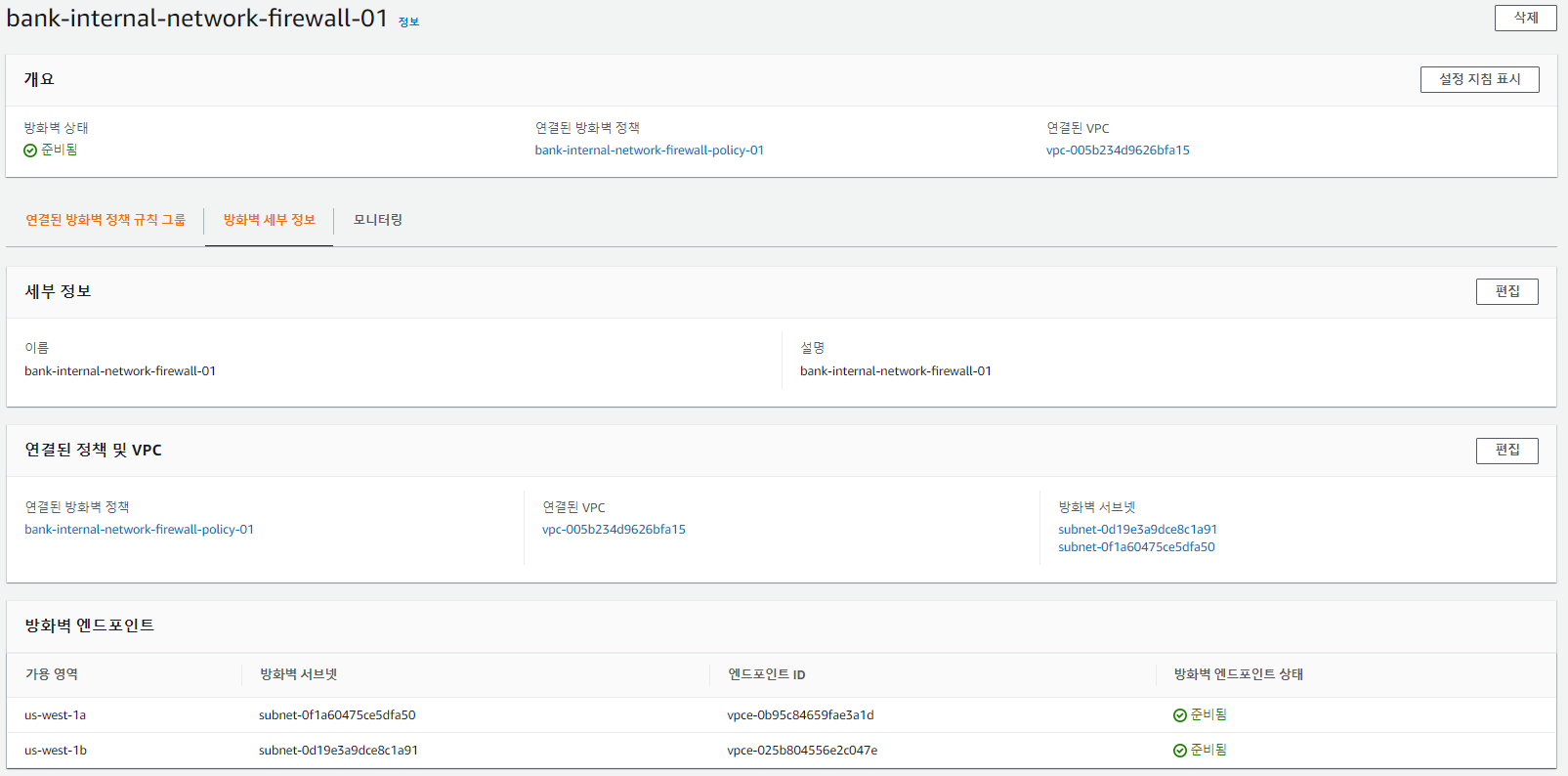
### 네트워크 방화벽 정책

|  |  |
| --- | --- |
| **네트워크 방화벽 정책 이름** | **상태 저장 규칙 그룹** |
| bank-internal-network-firewall-policy-01 | bank-internal-network-firewall-rg-01 |



### 네트워크 방화벽

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **네트워크 방화벽 이름** | **방화벽 정책** | **가용영역** | **서브넷** | **VPC** |
| bank-internal-network-firewall-01 | bank-internal-network-firewall-policy-01 | us-west-1a us-west-1b | bank-internal-edge-subnet-01 bank-internal-edge-subnet-02 | bank-external-vpc-01 |



## bank-internal-edge- subntet-01

### 키페어

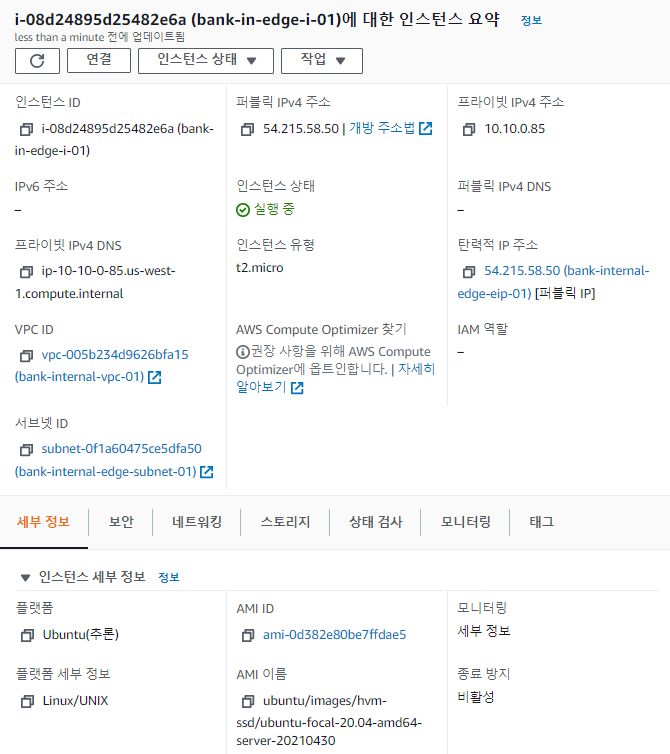
|  |  |
| --- | --- |
| **키 페어 이름** | **유형** |
| bank-in-edge-key-01 | RSA(.ppk) |



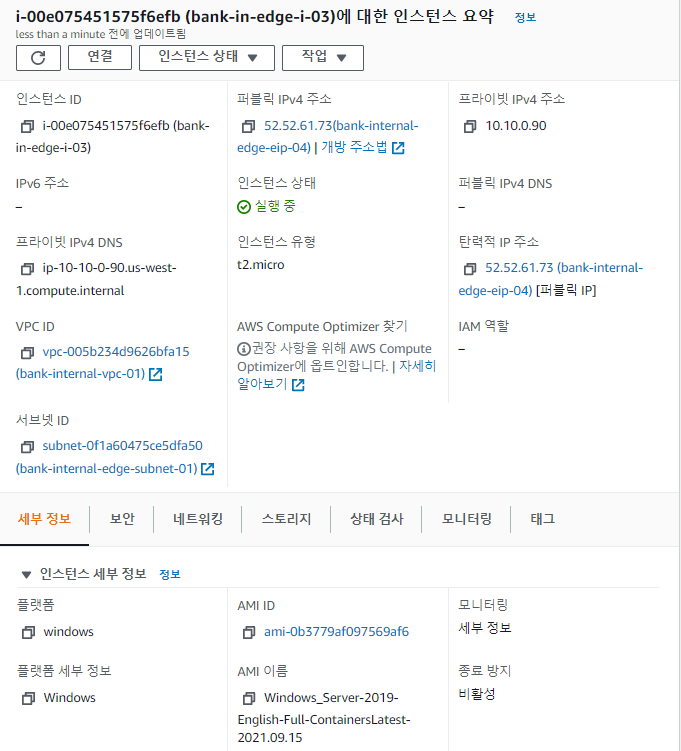
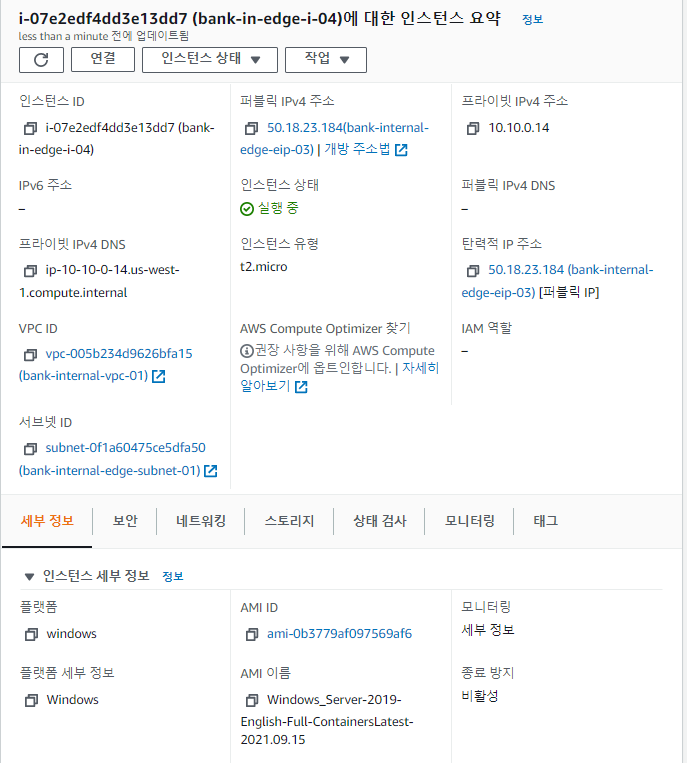
### 인스턴스

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **탄력적 IP 주소 이름** | **인스턴스 이름** | **키 페어 이름** | **보안 그룹 이름** | **서브넷 이름** |
| bank-internal-edge-eip-01 | bank-in-edge-i-01 | bank-in-edge-key-01 | bank-internal-edge-sg-01(default) | bank-internal-edge-subnet-01 |
| bank-internal-edge-eip-02 | bank-in-edge-i-02 | bank-in-edge-key-01 | bank-internal-edge-sg-01(default) | bank-internal-edge-subnet-01 |
| bank-internal-edge-eip-03 | bank-in-edge-i-03 | bank-in-edge-key-01 | bank-internal-edge-sg-01(default) | bank-internal-edge-subnet-01 |
| bank-internal-edge-eip-04 | bank-in-edge-i-04 | bank-in-edge-key-01 | bank-internal-edge-sg-01(default) | bank-internal-edge-subnet-01 |

Ubuntu Server 20.04 / 64비트 / 8GB



Windows Server 2019 / 64비트 / 30GiB

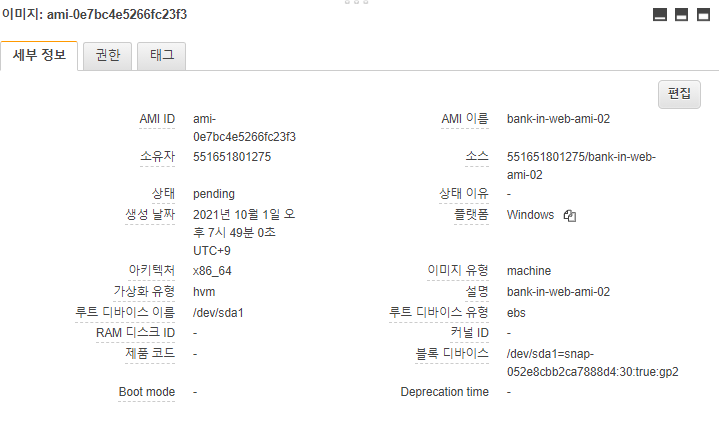
 

## bank-internal-web- subntet-01

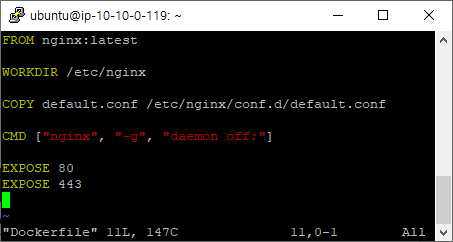
### AMI

|  |
| --- |
| **AMI 이름** |
| bank-in-web-ami-01 |
| bank-in-web-ami-02 |

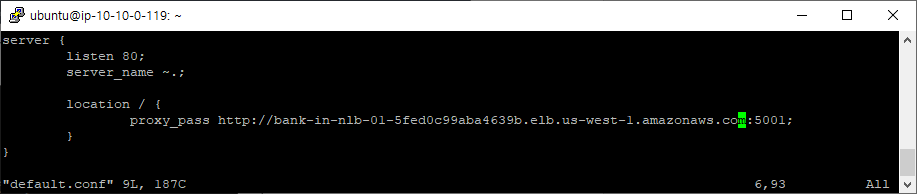




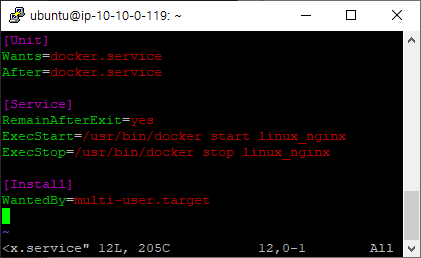
##### 내부(직원용) CRM Web – Dockerfile



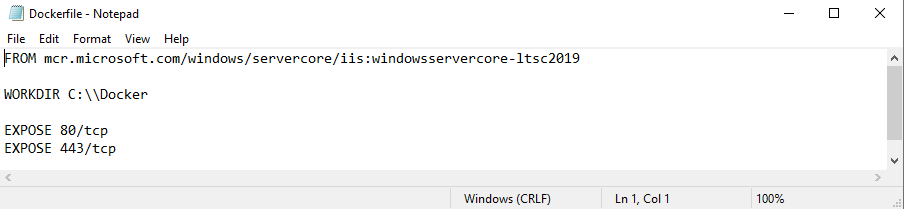
##### 내부(직원용) CRM Web – default.conf



##### 내부(직원용) CRM Web – /etc/system/system/linux\_nginx.service



##### 내부(직원용) Groupware Web – Dockerfile



##### 내부(직원용) Groupware Web – --restart=always



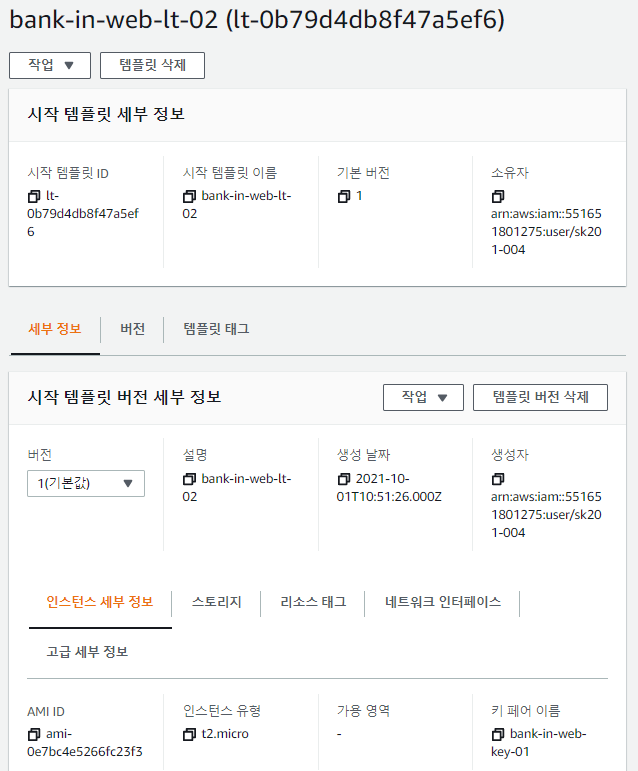
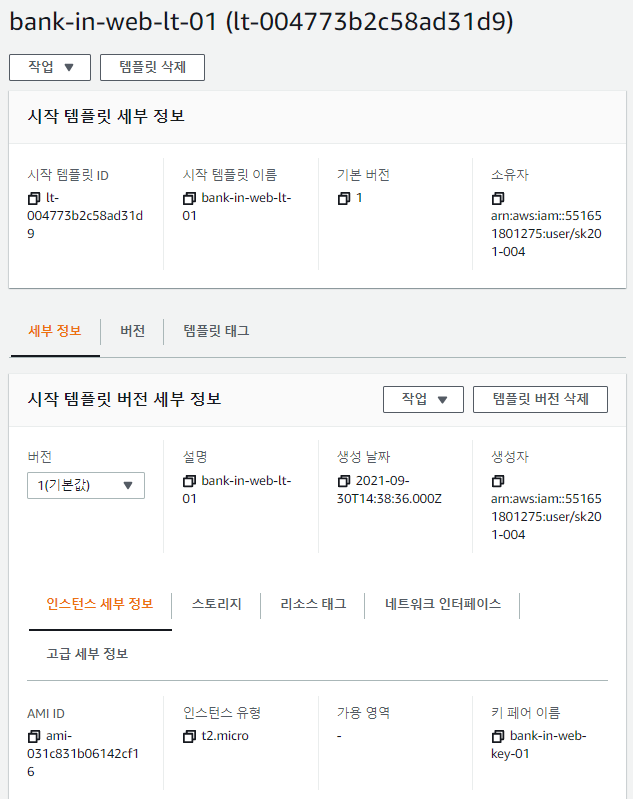
### 키페어

|  |  |
| --- | --- |
| **키 페어 이름** | **유형** |
| bank-in-web-key-01 | RSA(.ppk) |



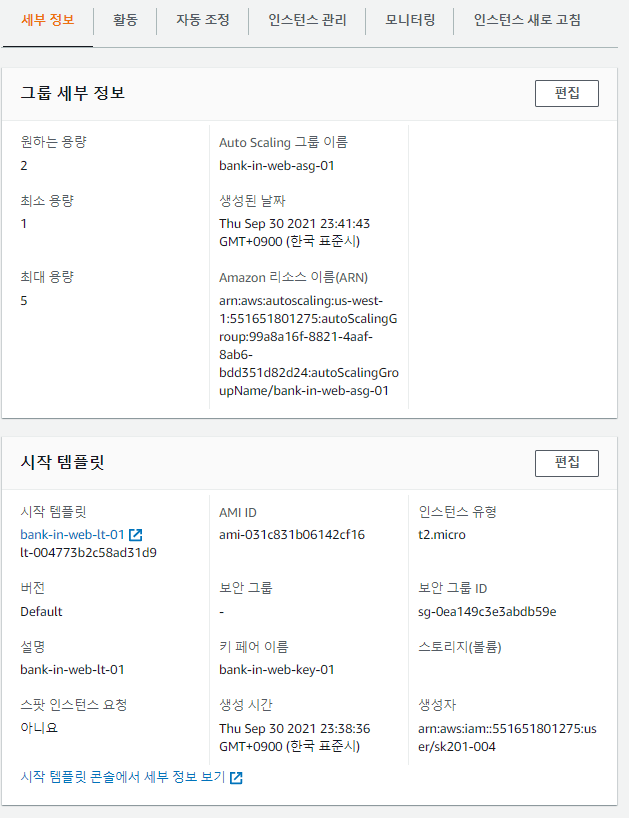
### 시작 템플릿

|  |  |  |
| --- | --- | --- |
| **시작 템플릿 이름** | **키 페어 이름** | **보안 그룹 이름** |
| bank-in-web-lt-01 | bank-in-web-key-01 | bank-internal-web-sg-01 |
| bank-in-web-lt-02 | bank-in-web-key-01 | bank-internal-web-sg-01 |



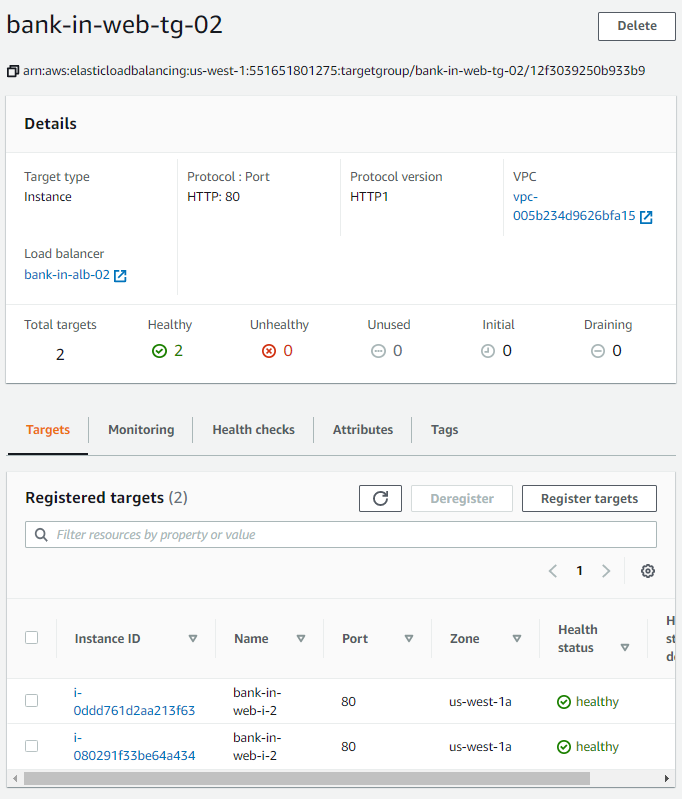
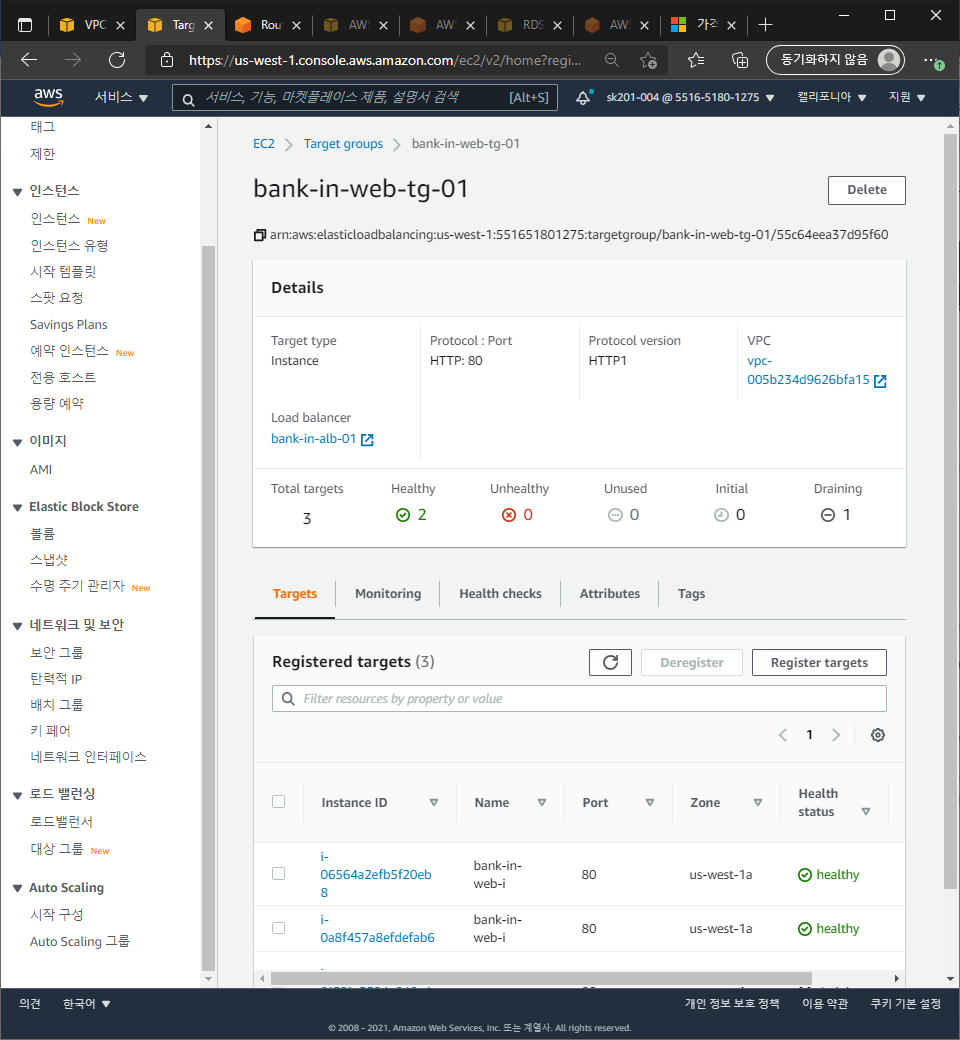
### Auto Scaling 그룹

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Auto Scaling 그룹 이름** | **시작템플릿/구성** | **원하는 용량** | **최소** | **최대** | **로드밸런서 대상 그룹** | **가용 영역** | **서브넷 이름** |
| bank-in-web-asg-01 | bank-in-web-lt-01 | 2 | 1 | 5 | bank-in-web-tg-01 | us-west-1a | bank-internal-web-subnet-01 |
| bank-in-web-asg-02 | bank-in-web-lt-02 | 2 | 1 | 5 | bank-in-web-tg-02 | us-west-1a | bank-internal-web-subnet-01 |



### 대상 그룹

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 대상 그룹 이름 | **Target** | **Target type** | **Protocol : Port** | **Load balancer** | **VPC** |
| bank-in-web-tg-01 | bank-in-web-i | Instance | HTTP : 80 | bank-in-alb-01 | bank-internal-vpc-01 |
| bank-in-web-tg-02 | bank-in-web-i-2 | Instance | HTTP : 80 | bank-in-alb-02 | bank-internal-vpc-01 |



### 로드밸런서

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 로드밸런서 이름 | **유형** | **체계** | **리스너 Protocol : Port - 대상** | **보안 그룹 이름** | **가용 영역** | **서브넷 이름** | **VPC** 이름 |
| bank-in-alb-01 | application | internet-facing | HTTP : 80 - 443 리디렉트 HTTPS : 443 - bank-ex-web-tg-01 | bank-internal-alb-sg-01 | us-west-1a us-west-1b | bank-internal-edge-subnet-01 bank-internal-edge-subnet-02 | bank-internal-vpc-01 |
| bank-in-alb-02 | application | internet-facing | HTTP : 80 - 443 리디렉트 HTTPS : 443 - bank-ex-web-tg-02 | bank-internal-alb-sg-01 | us-west-1a us-west-1b | bank-internal-edge-subnet-01 bank-internal-edge-subnet-02 | bank-internal-vpc-01 |





## bank-internal-was- subntet-01

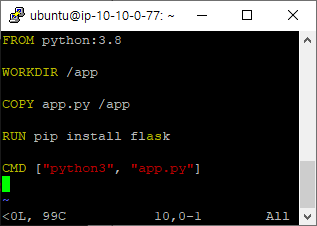
### AMI

|  |
| --- |
| **AMI 이름** |
| bank-in-was-ami-01 |
| bank-in-was-ami-02 |

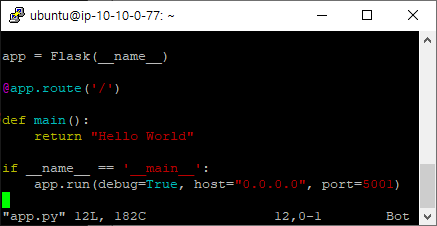




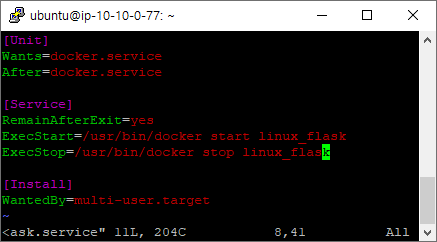
##### 내부(직원용) CRM WAS - Dockerfile



##### 외부(직원용) CRM WAS - app.py



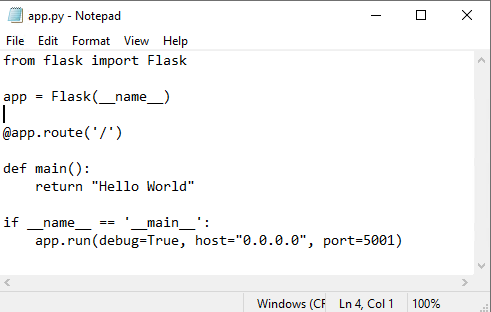
##### 외부(직원용) CRM WAS – /etc/system/system/linux\_flask.service



##### 내부(직원용) Groupware WAS - Dockerfile



##### 내부(직원용) Groupware WAS – app.py



##### 내부(직원용) Groupware WAS – --restart=always



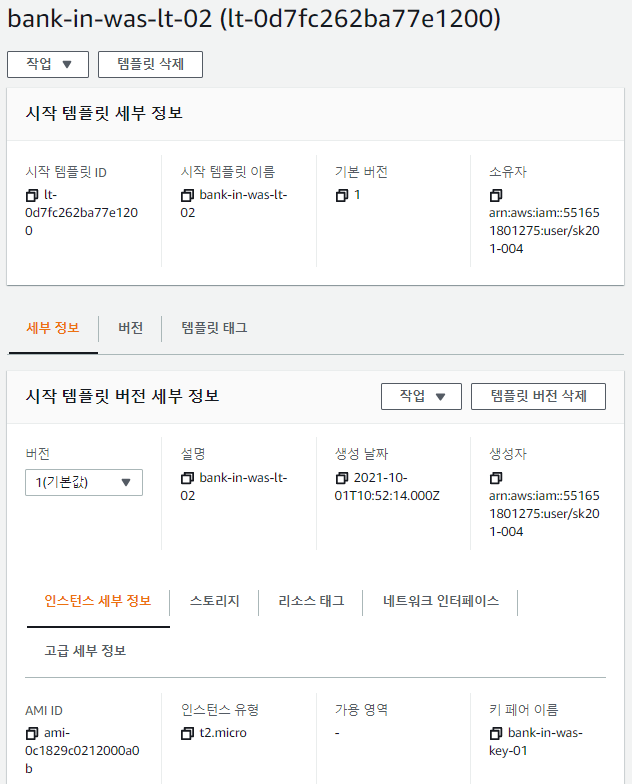
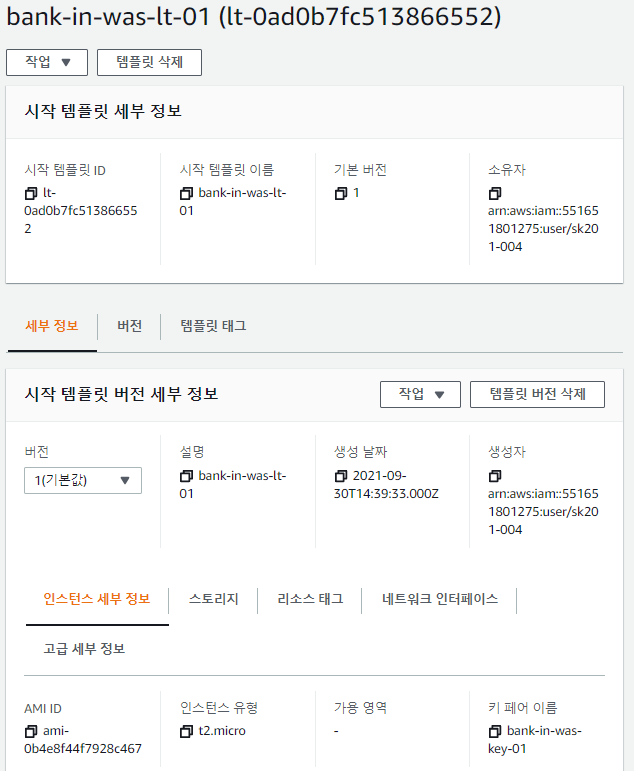
### 키페어

|  |  |
| --- | --- |
| **키 페어 이름** | **유형** |
| bank-in-was-key-01 | RSA(.ppk) |



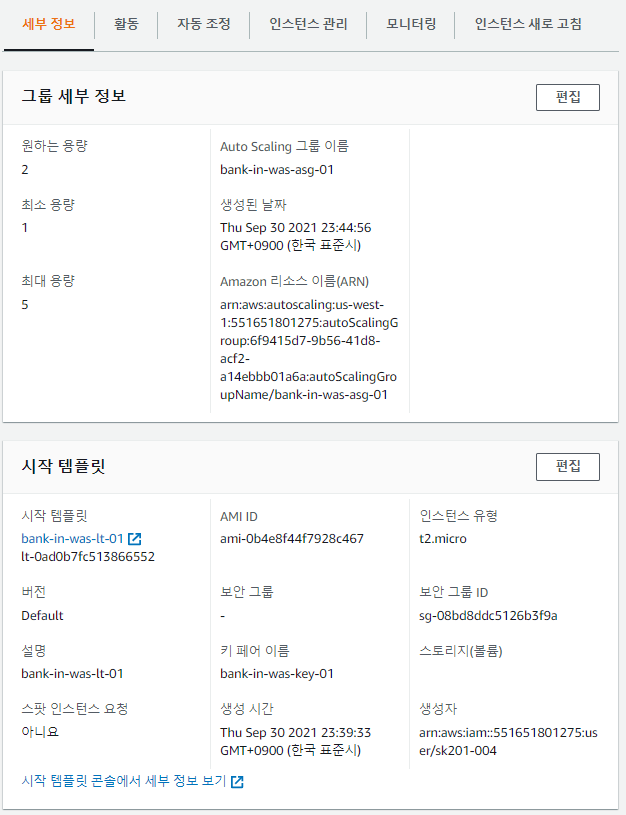
### 시작 템플릿

|  |  |  |
| --- | --- | --- |
| **시작 템플릿 이름** | **키 페어 이름** | **보안 그룹 이름** |
| bank-in-was-lt-01 | bank-in-was-key-01 | bank-internal-was-sg-01 |
| bank-in-was-lt-02 | bank-in-was-key-01 | bank-internal-was-sg-01 |



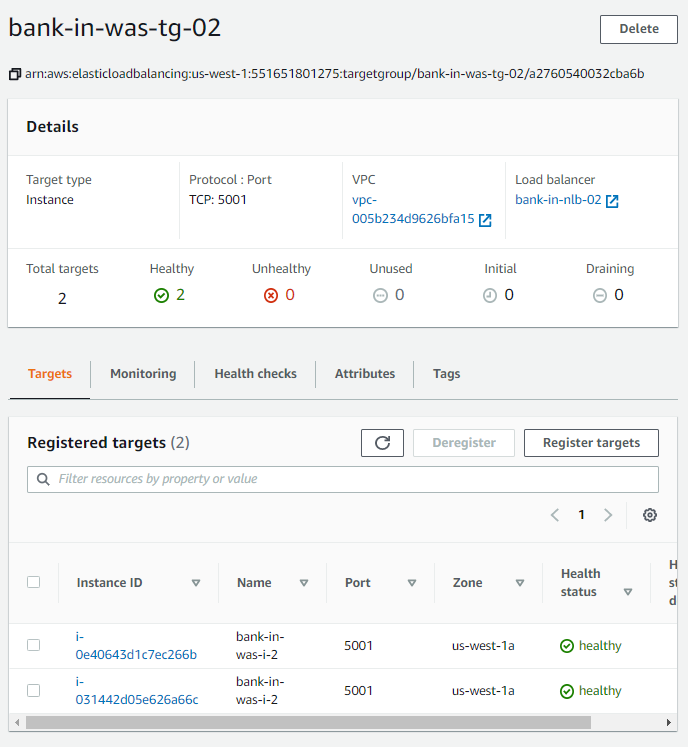
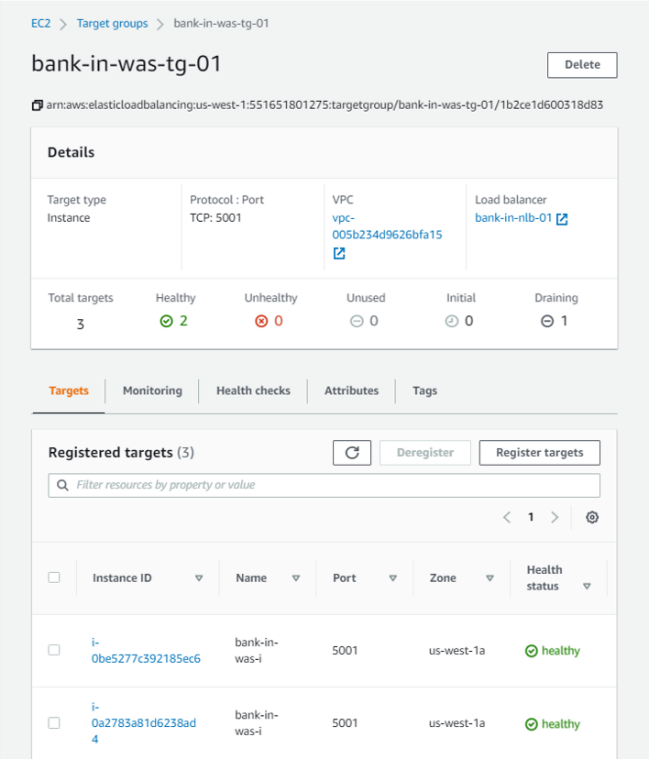
### Auto Scaling 그룹

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Auto Scaling 그룹 이름** | **시작템플릿/구성** | **원하는 용량** | **최소** | **최대** | **로드밸런서 대상그룹** | **가용 영역** | **서브넷 이름** |
| bank-in-was-asg-01 | bank-in-was-lt-01 | 2 | 1 | 5 | bank-in-was-tg-01 | us-west-1a | bank-internal-was-subnet-01 |
| bank-in-was-asg-02 | bank-in-was-lt-02 | 2 | 1 | 5 | bank-in-was-tg-02 | us-west-1a | bank-internal-was-subnet-01 |



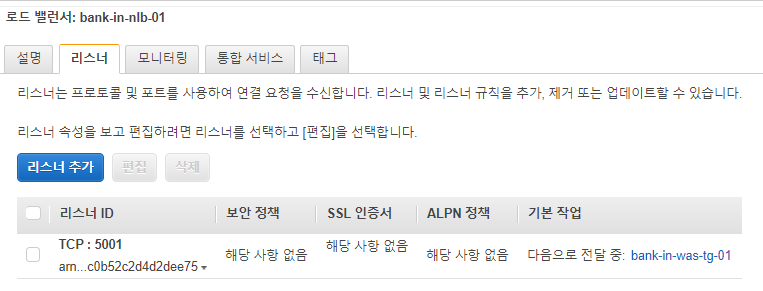
### 대상 그룹

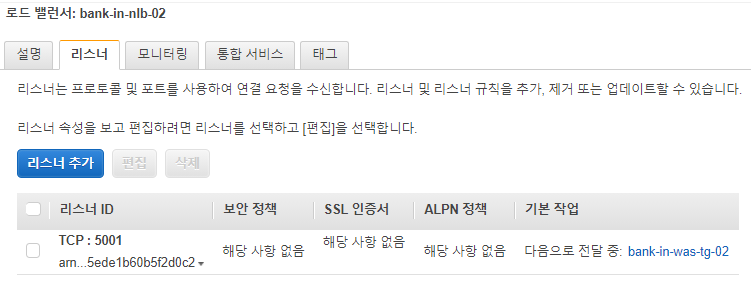
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 대상 그룹 이름 | **Target** | **Target type** | **Protocol : Port** | **Load balancer** | **VPC** |
| bank-in-was-tg-01 | bank-in-was-i | Instance | TCP : 5001 | bank-in-nlb-01 | bank-internal-vpc-01 |
| bank-in-was-tg-02 | bank-in-was-i-2 | Instance | TCP : 5001 | bank-in-nlb-02 | bank-internal-vpc-01 |



### 로드밸런서

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 로드밸런서 이름 | **유형** | **체계** | **리스너 Protocol : Port - 대상** | **가용 영역** | **서브넷 이름** | **VPC** 이름 |
| bank-in-nlb-01 | network | internal | TCP : 5001 | us-west-1a | bank-internal-was-subnet-01 | bank-internal-vpc-01 |
| bank-in-nlb-02 | network | internal | TCP : 5001 | us-west-1a | bank-internal-was-subnet-01 | bank-internal-vpc-01 |

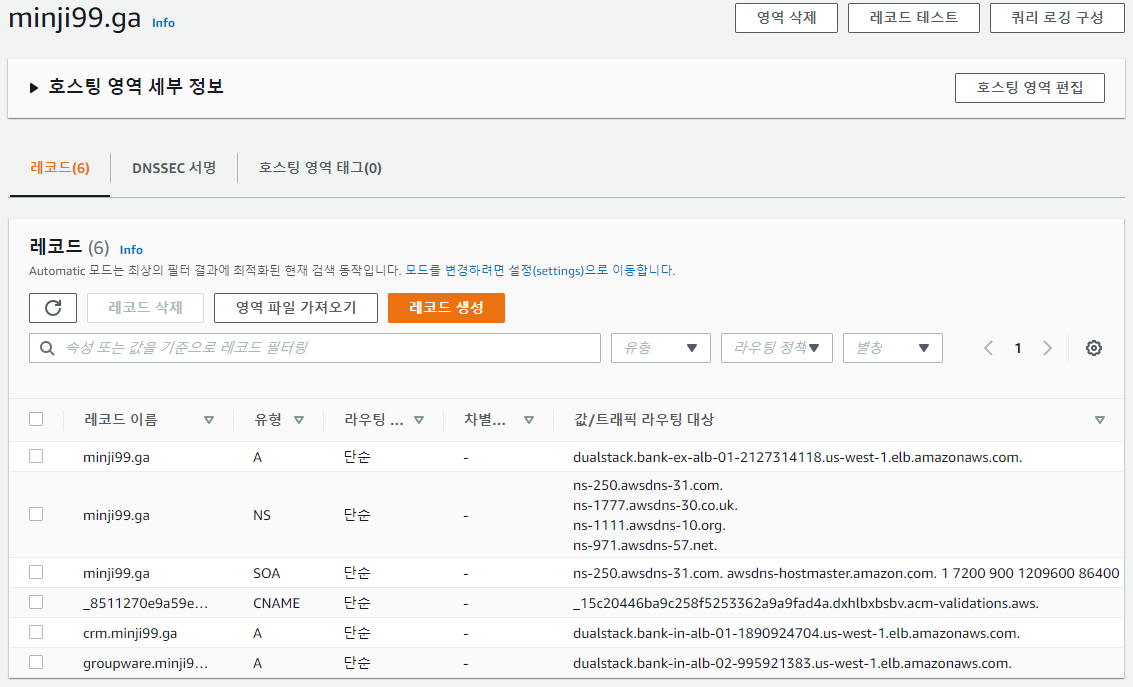




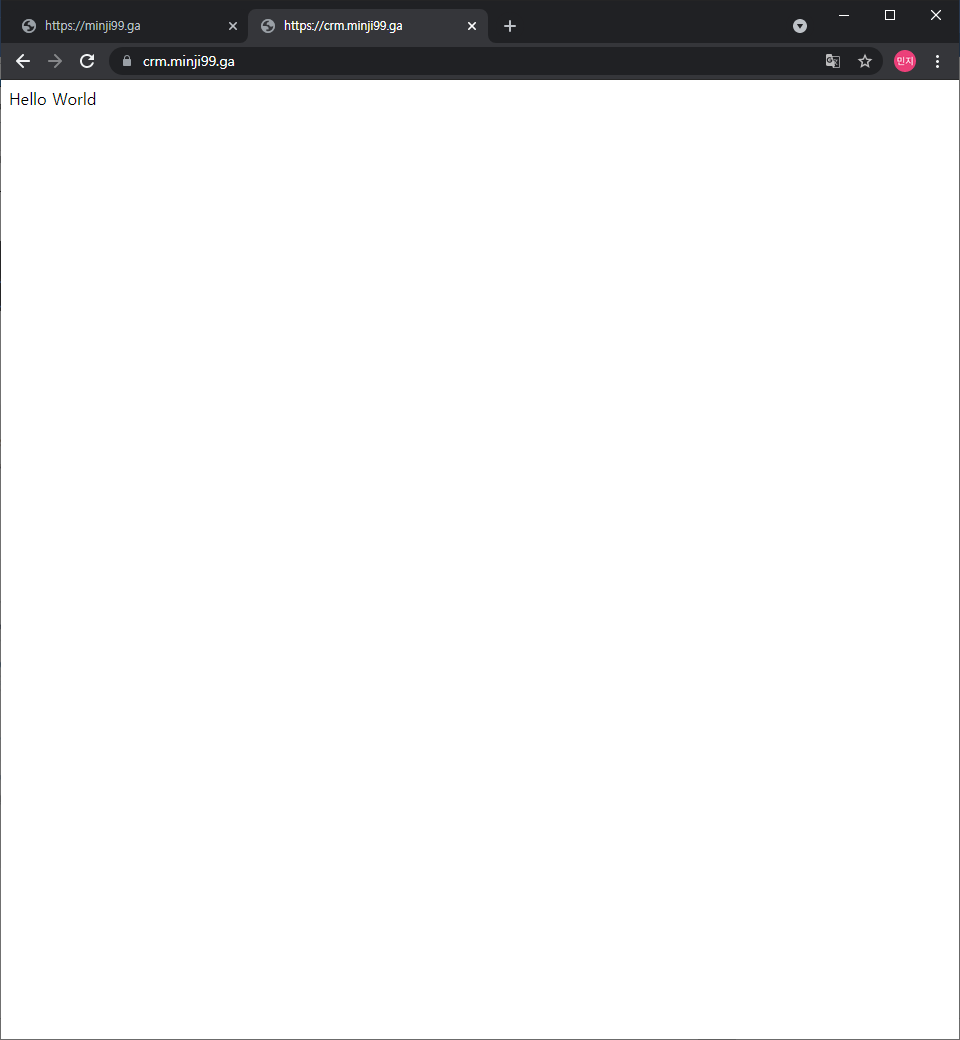
## Route53

### 호스팅 영역

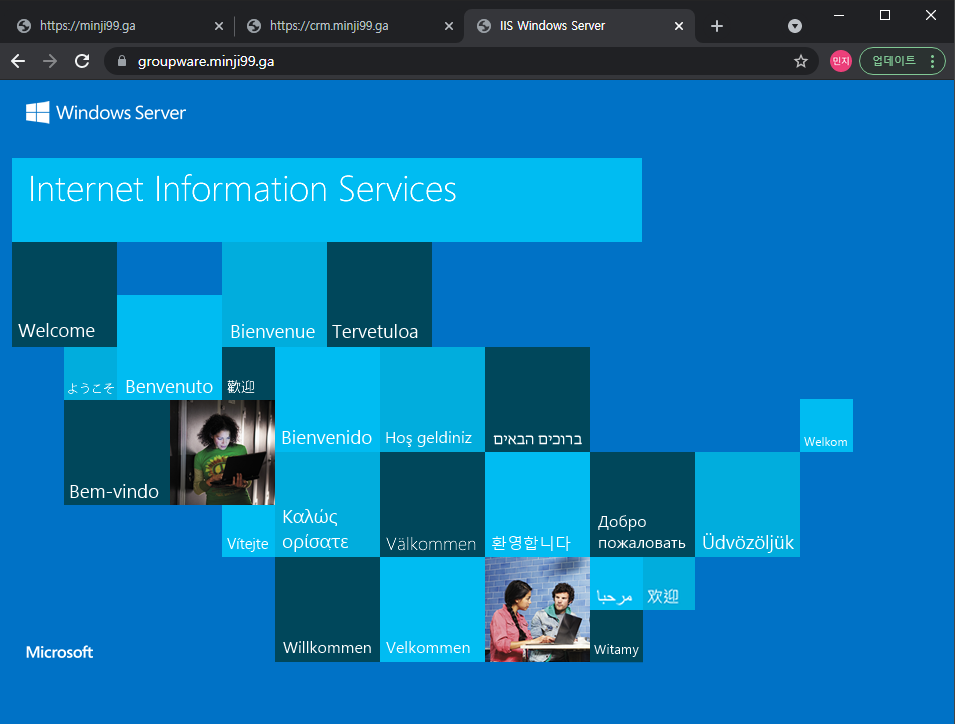
|  |  |  |
| --- | --- | --- |
| **도메인 이름** | **유형** | **레코드: 레코드 이름 - 유형 - 값/트래픽 라우팅 대상** |
| minji99.ga | 퍼블릭 | minji99.ga - NS - ns-81.awsdns-10.com. minji99.ga - NS - ns-1858.awsdns-40.co.uk. minji99.ga - NS - ns-882.awsdns-46.net. minji99.ga - NS - ns-1448.awsdns-53.org.  minji99.ga - SOA - ns-81.awsdns-10.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400  \_8511270e9a59e2f4a299f5bb8c9cd7fe.minji99.ga - CNAME - \_15c20446ba9c258f5253362a9a9fad4a.dxhlbxbsbv.acm-validations.aws.  minji99.ga - A - dualstack.bank-ex-alb-01-1622078044.us-west-1.elb.amazonaws.com.  crm.minji99.ga - A - dualstack.bank-in-alb-01-1187725526.us-west-1.elb.amazonaws.com.  groupware.minji99.ga - A - dualstack.bank-in-alb-02-995921383.us-west-1.elb.amazonaws.com. |



##### 내부(직원용) CRM Web 및 WAS 연동



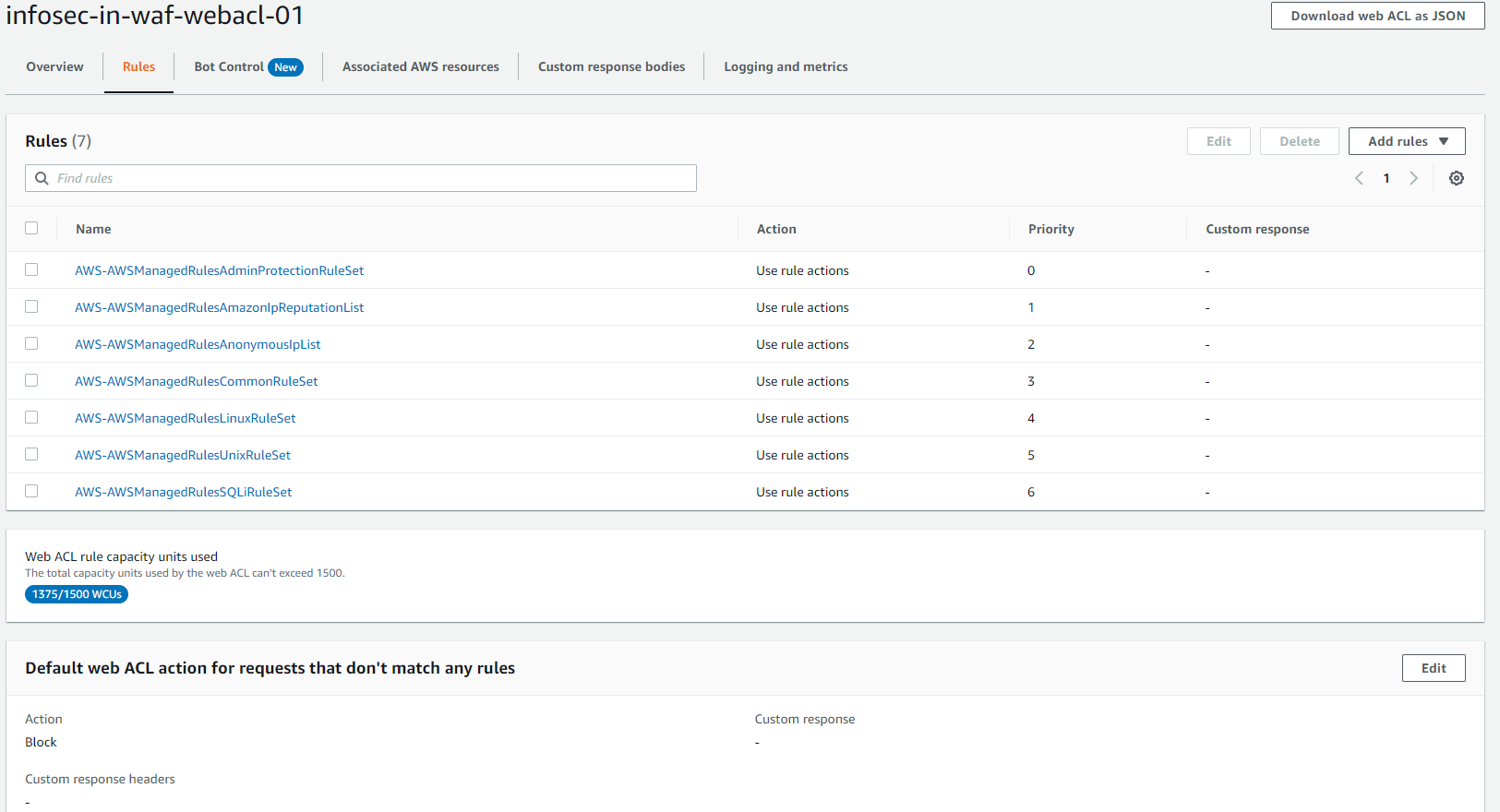
##### 내부(직원용) Groupware Web 및 WAS 연동 미해결



## WAF & Shield

### Web ACLs

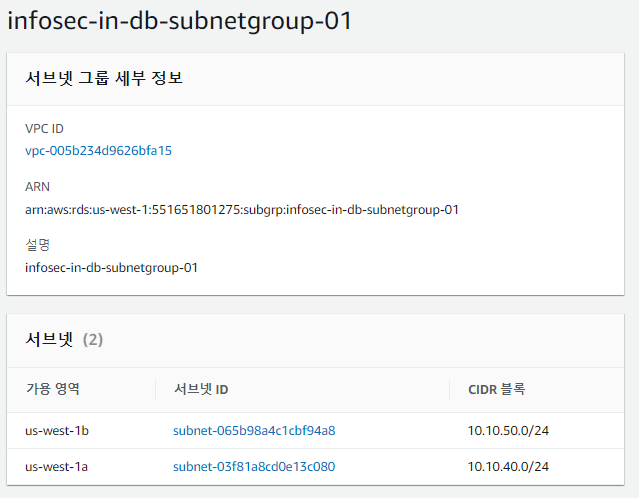
|  |  |  |  |
| --- | --- | --- | --- |
| **Web ACLs 이름** | **Rules: Priority: Name - Action** | **Default web ACL action for requests that don't match any rules** | **Associated AWS resources: Name - Resource type -Region** |
| infosec-in-waf-webacl-01 | 0: AWS-AWSManagedRulesAdminProtectionRuleSet - Use rule actions 1: AWS-AWSManagedRulesAmazonIpReputationList - Use rule actions 2: AWS-AWSManagedRulesAnonymousIpList - Use rule actions 3: AWS-AWSManagedRulesCommonRuleSet - Use rule actions 4: AWS-AWSManagedRulesLinuxRuleSet - Use rule actions 5: AWS-AWSManagedRulesUnixRuleSet - Use rule actions 6: AWS-AWSManagedRulesSQLiRuleSet - Use rule actions | Block | bank-in-alb-01 - Application Load Balancer -US West (N. California) bank-in-alb-02 - Application Load Balancer -US West (N. California) |



## bank-internal-db-subntet-01 & bank-internal-db-subntet-02

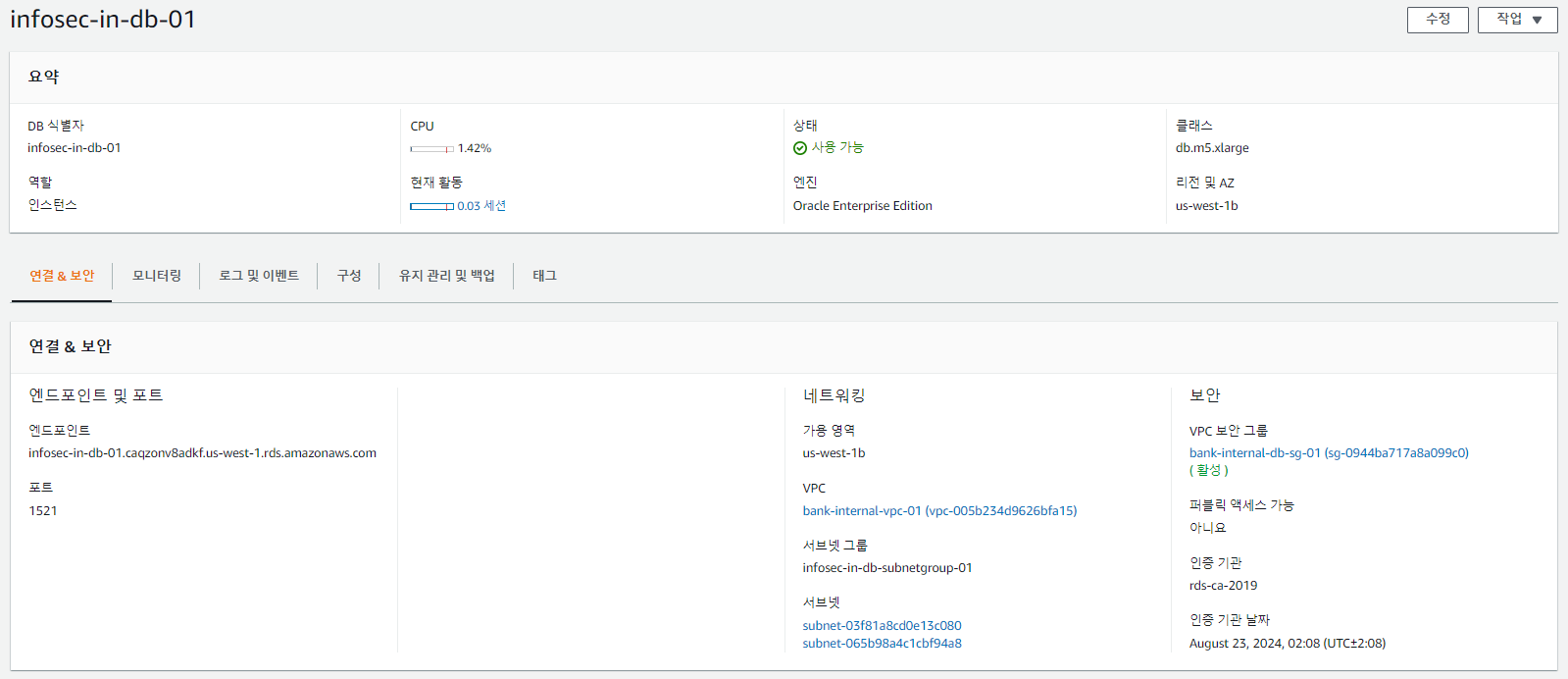
### 서브넷 그룹

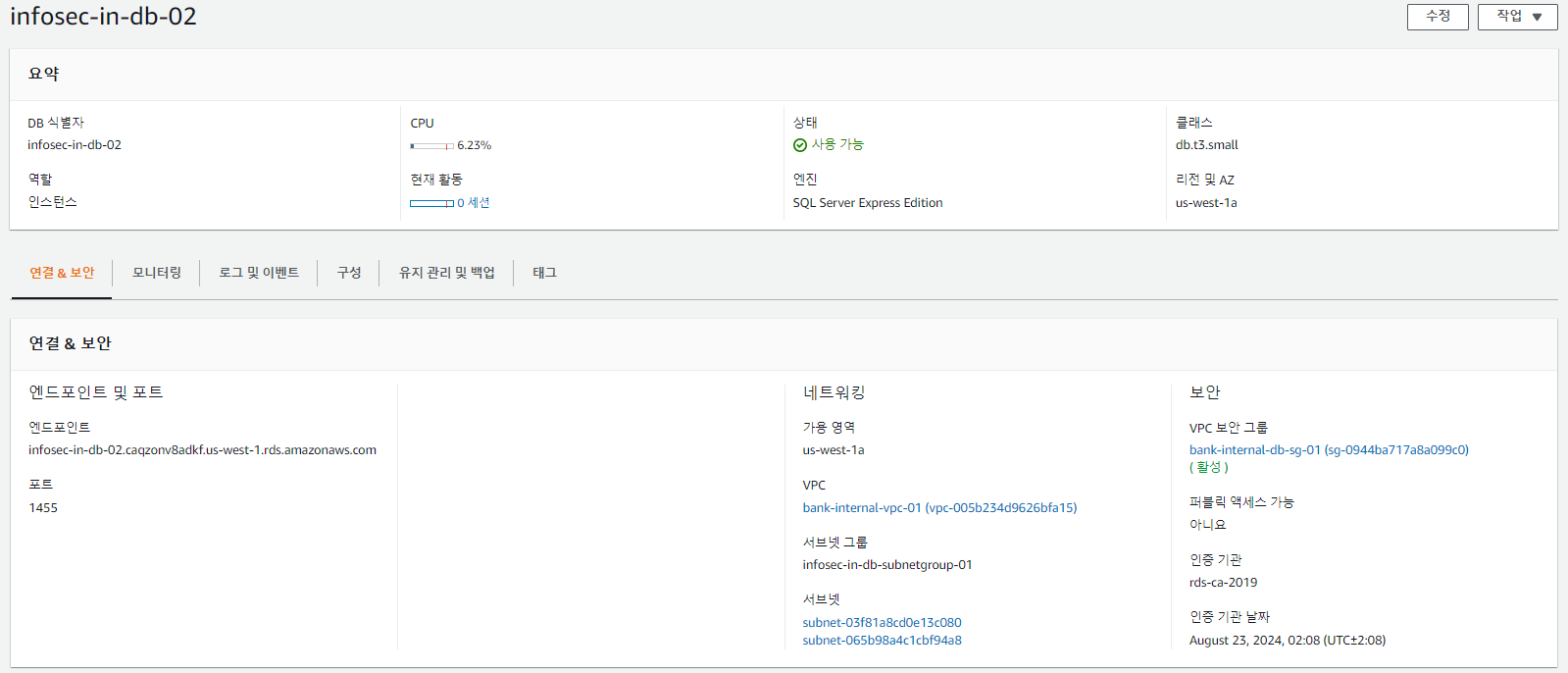
|  |  |  |
| --- | --- | --- |
| **서브넷 그룹 이름** | **서브넷 이름** | **IP(CIDR)** |
| infosec-in-db-subnetgroup-01 | infosec-internal-db-subnet-01 infosec-internal-db-subnet-02 | 10.10.40.0/24 10.10.50.0/24 |



### 데이터베이스

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **DB 이름** | **역할** | **포트** | **가용 영역** | **보안 그룹 이름** | **서브넷 그룹 이름** | **VPC 이름** |
| infosec-in-db-01 | 인스턴스 | 1521 | us-west-1b | bank-internal-db-sg-01 | infosec-in-db-subnetgroup-01 | bank-internal-vpc-01 |
| infosec-in-db-01(복제) | 인스턴스 |  | us-west-1b |  |  |  |
| infosec-in-db-02 | 인스턴스 | 1455 | us-west-1a | bank-internal-db-sg-01 | infosec-in-db-subnetgroup-01 | bank-internal-vpc-01 |
| infosec-in-db-02(복제) | 인스턴스 |  | us-west-1a |  |  |  |





# 구성하면서 발생했던 오류

* nslookup으로 도메인 안뜨는 이유: Freenom에 AWS Route53의 ns 필드를 입력 안했기 때문
* 인증서 – www.minji99.ga는 주의 요함: minji99.ga 인증서 O / www.minji99.ga 인증서 X

\*.minji99.ga로 인증서 재발급하면 www도 보호가능

* 대상그룹에 대상이 없을 때 503 service temporarily unavailable
* 로드밸런서 443 대상그룹 80이 아니면 502 bad gateway: 443으로 들어와서 nginx의 80 서비스 이용,

nginx에서 직접 443 listen 안하는 이유: ACM에서 발급받은 인증서는 사설인증서가 아니여서 내보내기가 안되기 때문

* 각 서브넷 nacl 아웃바운드 설정 안하면 504 gateway time-out: 나갈 길이 없기 때문
* 윈도우 서버에서 도커를 사용하기 위해서는 Windows 기반 컨테이너를 이용해야 함

# 구성하면서 알게된 점

* 고가용성 - 클러스터, 복제
  + Aurora DB는 다른 region에 리더 인스턴스가 생성 (클러스터)
  + Oracle DB는 같은 region에 복제본 인스턴스가 생성 (복제)
  + MS SQL DB는 같은 region에 복제본 인스턴스가 생성 (복제)
  + Oracle DB & MS SQL DB를 같은 서브넷 그룹으로 생성시 다른 region에 생성 가능
* 네트워크 방화벽 하나 생성 시 여러 region 당 하나의 서브넷으로 방화벽 배포 가능
* WAF의 Web ACLs 생성 시 ALB(resources) 선택 가능

# 추가 실습(모듈프로젝트2 + AWS 연동)



# 향후 과제

* 내부(직원용) Groupware Web(IIS) 및 WAS(Flask) 연동
* WAS 및 DB 연동
* 피어링 연결
* 사이트 간 VPN 연결 (Site-to-site VPN)
* Cloud Trail
* ECS, ECR, Fargate
* 보안: 네트워크 ACL, 보안그룹, WAF 룰셋 설정