업무참고 2025-클라우드대응-②-62

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서

ORACLE

금융보안원
FINANCIAL SECURITY INSTITUTE

ORACLE

CONTENTS

1. 가상 자원 관리

1.1. 가상 자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립
1.2. 이용자 가상 자원 접근 시 로그인 규칙 적용
1.3. 가상 자원 루트 계정 접근 시 추가 인증수단 적용
1.4. 가상 자원 생성 시 네트워크 설정 적용
1.5. 가상 자원 접속 시 보안 방안 수립
1.6. 이용자 가상 자원 별 권한 설정
1.7. 이용자 가상 자원 내 악성코드 통제방안 수립

1 가상 자원 관리

1 기준

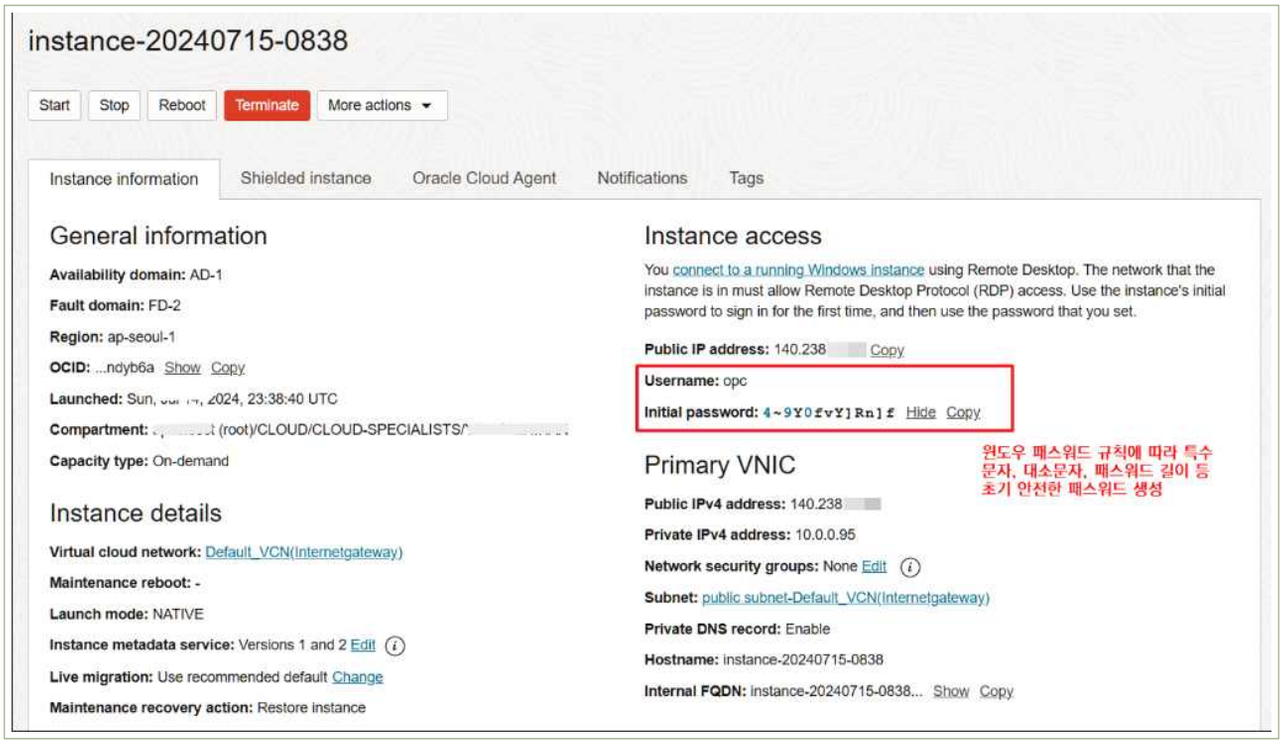
식별번호	기준	내용
1.1	**가상 자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립**	이용자 가상 자원 생성 시 최초 계정에 대한 비밀번호 규칙을 수립하여야 한다.

2 설명

- 이용자 가상 자원에 접근하는 계정에 대한 비밀번호 규칙 보안 통제 방안을 수립하여야 한다.
  1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

3 우수 사례

- (OCI 콘솔) '홈' → 'Compute' → 'Instances' → 'Crete Instance'에서 Winodws 이미지 생성 시 Winodws 패스워드 생성 규칙에 따라 특수 문자, 길이, 복잡도 등이 포함된 최초 비밀번호가 생성되며, 이후 변경 시에도 동일한 패스워드 규칙을 적용
  - [Linux] Private Key 기반의 인증을 통한 접근 방식
  - [Windows] Windows 패스워드 규칙에 따라 안전한 패스워드 생성



| 그림 1.1.1 | 안전한 초기 패스워드 생성

4 참고 사항

- https://cloud.oracle.com/compute/instances?region=ap-seoul-1

1 기준

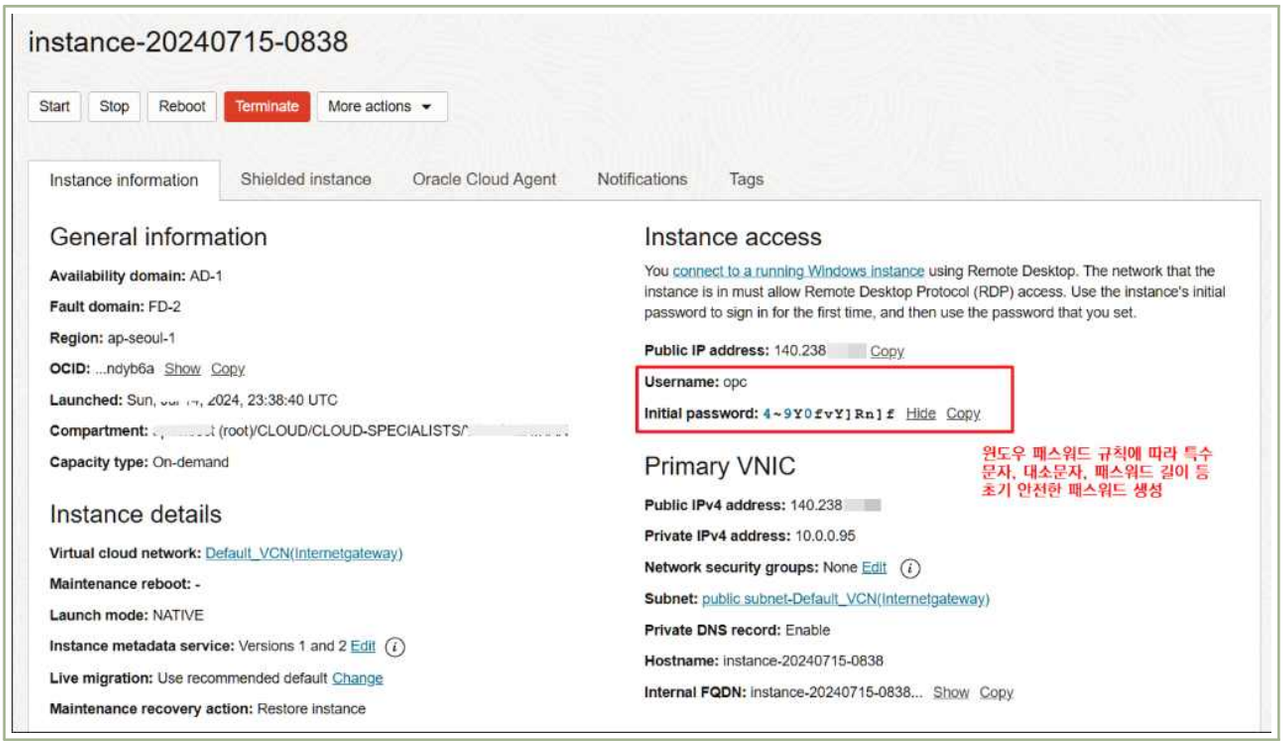
식별번호	기준	내용
1.2	**이용자 가상 자원 접근 시 로그인 규칙 적용**	이용자 가상 자원 접근 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.

2 설명

- 이용자는 패스워드 무작위 대입 공격 등에 대응하기 위해 가상 자원 접근 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.
  1) 로그인 오류에 따른 보안통제 방안 수립 등

3 우수 사례

- (OCI 콘솔) '홈' → 'Compute' → 'Instances' → 'Create Instance'에서 Windows 이미지 생성 시 Windows 비밀번호 규칙에 따라 특수 문자, 길이, 복잡도 등이 포함된 최초 비밀번호가 생성되며, Winodws 로그인 후 Password reset 과정을 통해 Winodws 비밀번호 규칙에 따라 안전한 패스워드 생성



| 그림 1.2.1 | 안전한 초기 패스워드 생성

4 참고 사항

- https://cloud.oracle.com/compute/instances?region=ap-seoul-1

※ 이후 본 문서에 기재되는 https://cloud.oracle.com으로 시작하는 모든 URL은 OCI 계정에 로그인한 상태에서만 접근 가능한 Oracle Cloud 콘솔 UI 참조 페이지입니다.

1 기준

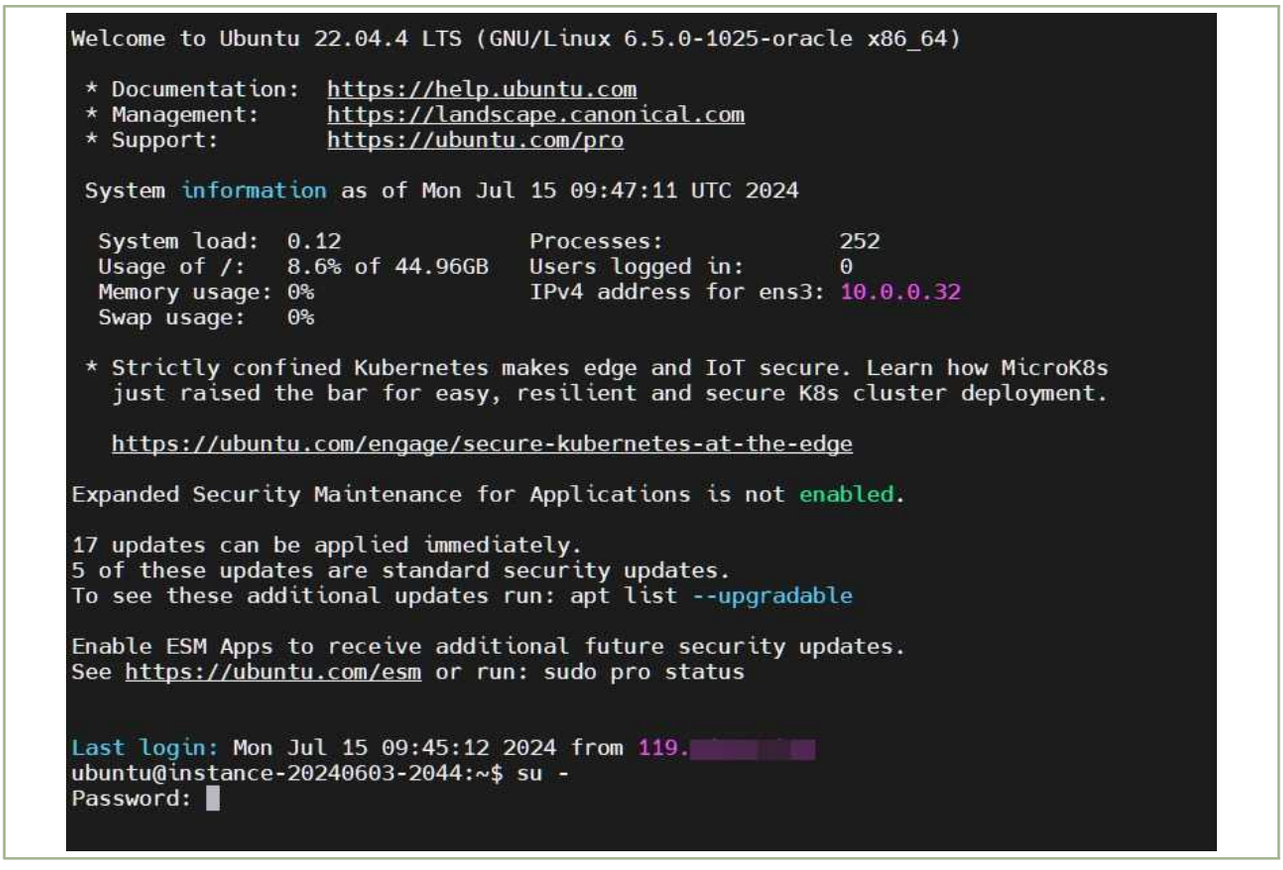
식별번호	기준	내용
1.3	**가상 자원 루트 계정 접근 시 추가 인증 수단 적용**	이용자 가상 자원 루트 계정(root, administrator 등) 접근 시 추가 인증 수단을 확보하여야 한다.

2 설명

- 이용자 가상 자원 루트 계정 접근 시 추가 인증 수단이 확보되어야 한다. (단, 기능이 제공되지 않는 경우 안전한 로그인 수단을 확보하여야 한다.
  1) 이메일 인증
  2) SMS 인증
  3) 별도 인증도구 활용
  4) SSH PEM KEY 등을 통한 안전한 로그인 수단 확보 등

3 우수 사례

- 일반 사용자 계정에서 루트(관리자) 계정에 접근할 때 sudo 또는 su 명령어를 실행하여 패스워드로 추가 인증을 해야 한다.



| 그림 1.3.1 | 패스워드 추가 인증

- [3rd party 솔루션 활용] OCI에서 가상머신의 루트 계정 접근 시 별도 추가 인증 수단은 제공하고 있지 않지만 가상 머신에 Google Authenticator와 같은 TOPT기반 2FA 적용하면 사용 가능함

1) Google Authenticator 설치

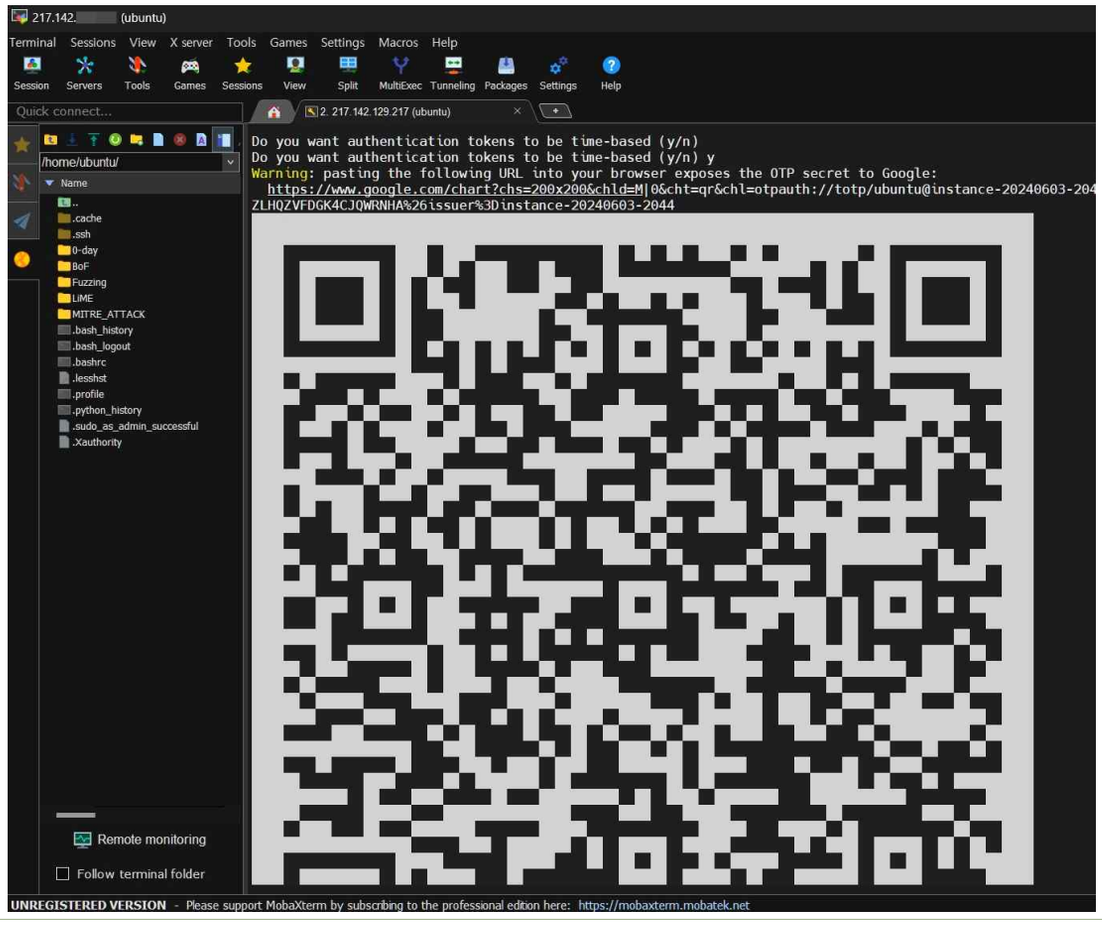
```
Bash
sudo apt-get update
sudo apt-get install libpam-google-authenticator
```

2) Google Authenticator 설정

- 각 사용자 계정에 대해 Google Authenticator를 설정

설정 과정에서 비밀 키와 QR코드를 받게 됩니다. 이를 Google Authenticator 앱에 추가

```
Bash
google-authenticator
```



| 그림 1.3.2 | QR코드 수신 화면

3) PAM 구성 파일 수정

- /etc/pam.d/sshd 파일을 열어 다음 줄을 추가

```
Bash
auth required pam_google_authenticator.so
```

4) SSH 데몬 설정 수정

- /etc/ssh/sshd_config 파일을 열어 다음 줄을 수정

```
Bash
ChallengeResponseAuthentication yes
```

5) SSH 데몬 재시작

```
Bash
sudo systemctl restart sshd
```

- Winodws의 경우 RDP 접속에 대한 2단계 인증(2FA) 설정을 위해서는 가상 자원에 DUO 클라이언트를 별도로 설치해 이용(https://duo.com/solutions)

1) DUO 계정 생성 및 설정
   DUO Security 웹사이트에서 계정을 생성하고 애플리케이션을 설정
2) DUO 클라이언트 설치
   Windows 가상 자원에 DUO 클라이언트 설치
3) DUO 설정
   https://duo.com/product/multi-factor-authentication-mfa

4 참고 사항

- DUO : https://duo.com/product/multi-factor-authentication-mfa

1 기준

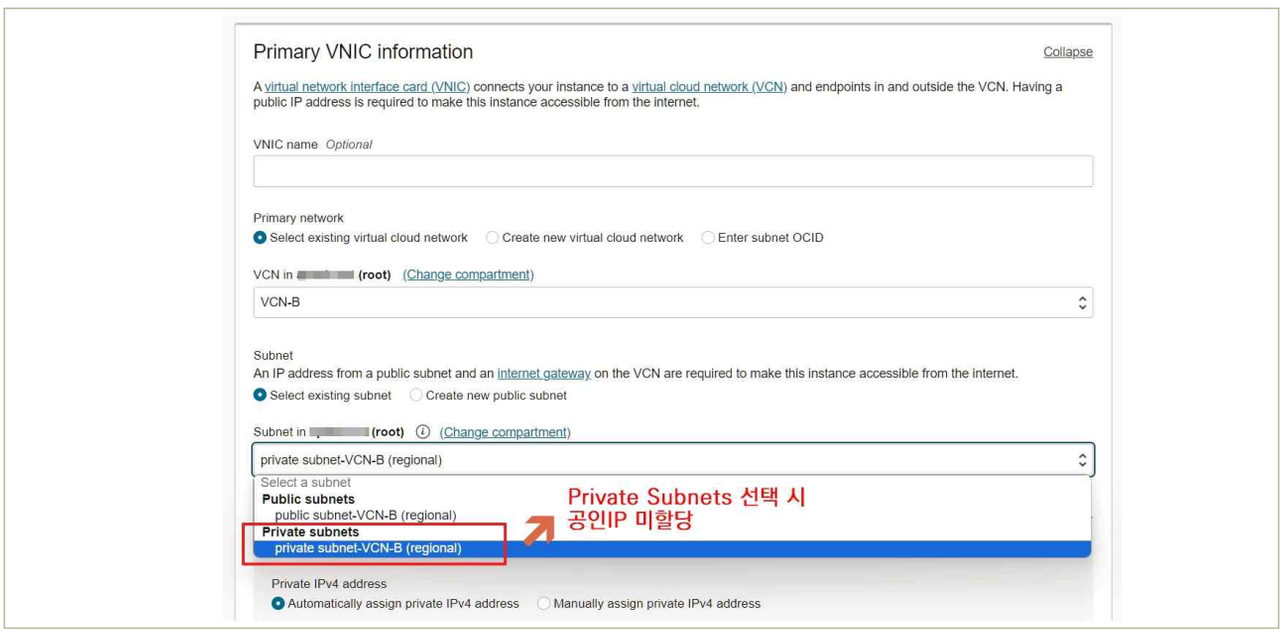
식별번호	기준	내용
1.4	**가상 자원 생성 시 네트워크 설정 적용**	이용자의 가상 자원 생성 시 안전한 네트워크 설정을 적용하여야 한다.

2 설명

- 외부에서 직접 접속이 불필요한 경우 내부 IP 또는 IP 대역에서만 접근할 수 있도록 설정하여야 한다.
  1) 가상 자원 접속이 가능한 공인 IP(외부) 대역 점검 및 제거
  2) 접근 가능한 IP 또는 대역대 설정
  3) VPC 및 보안 그룹을 통한 내부 네트워크 대역 접근 설정

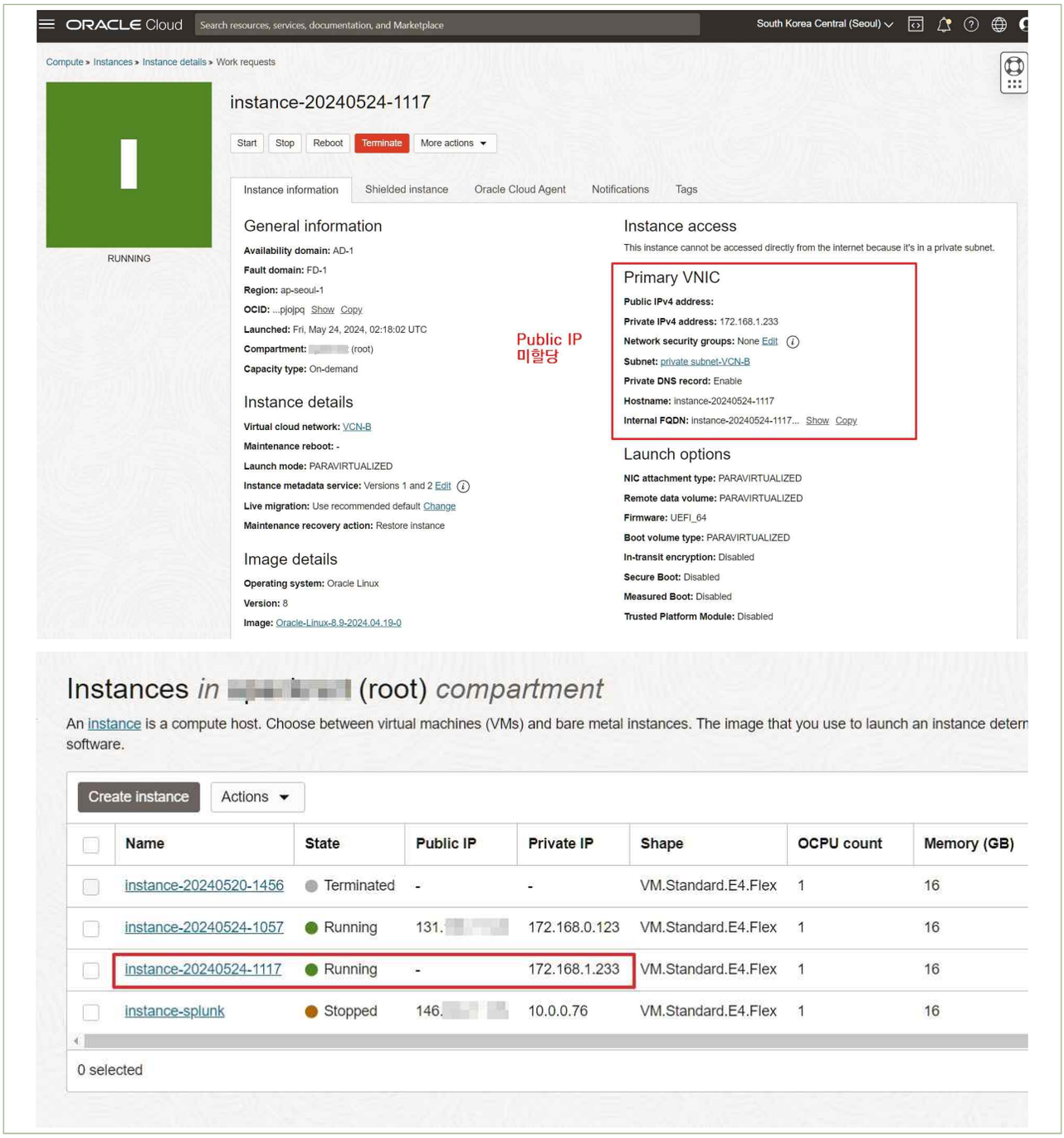
3 우수 사례

- (OCI 콘솔) '홈' → 'Compute' → 'Instances' → 'Create Instance'를 통해 인스턴스 생성 시 Private Subnet으로 구성하면 공인 IP를 할당할 수 없도록 리소스 구성 가능
  1) 가상 자원에 접속 가능한 공인 IP(외부) 대역을 점검하고 제거



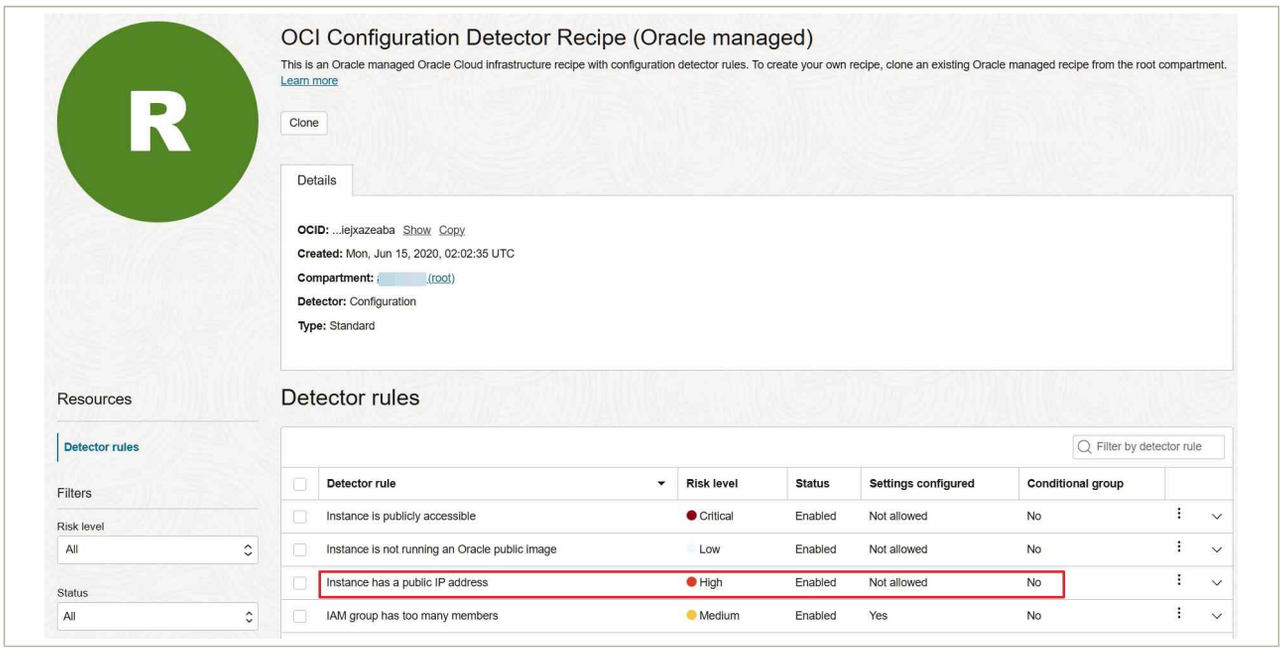
| 그림 1.4.1 | Private Subnet으로 네트워크 구성

- 생성된 인스턴스(Instance) VNIC에 공인 IP 할당하지 않고 리소스 구성 완료



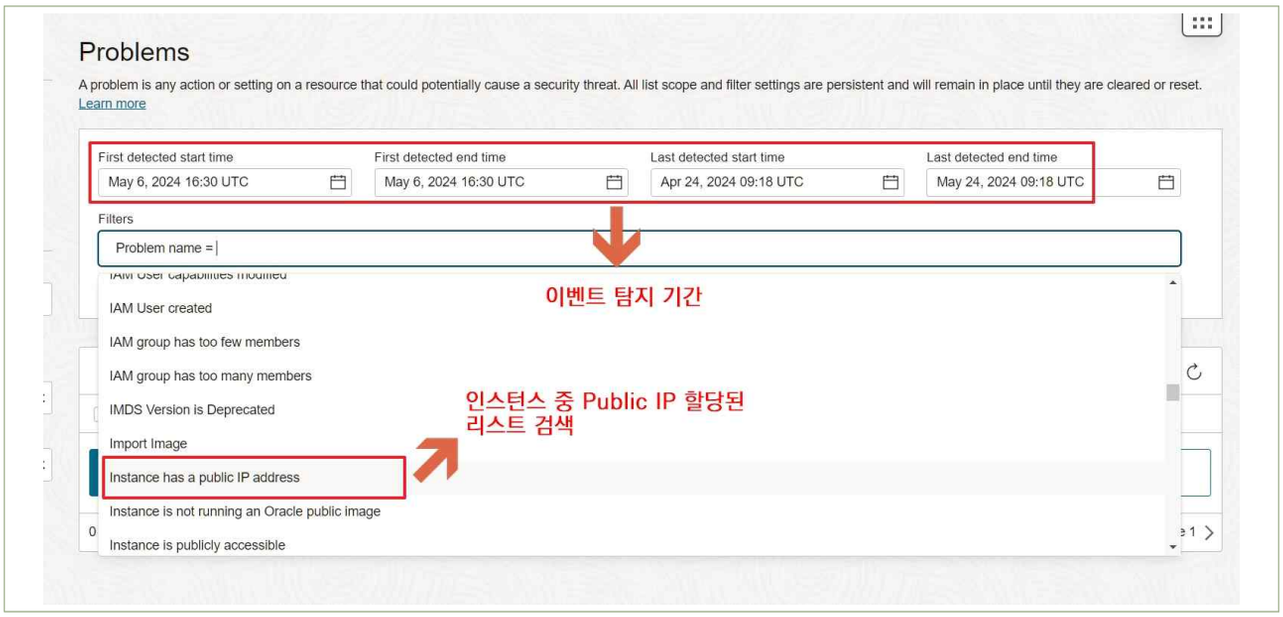
| 그림 1.4.2 | VNIC IP설정 화면

- 전체 인스턴스(Instance) 리소스 중 Public Subnet으로 구성되어 있는 항목 중 공인 IP(외부)로 잘못 할당된 인스턴스를 검색하기 위해서는 OCI Cloud Guard를 통해 확인 및 점검

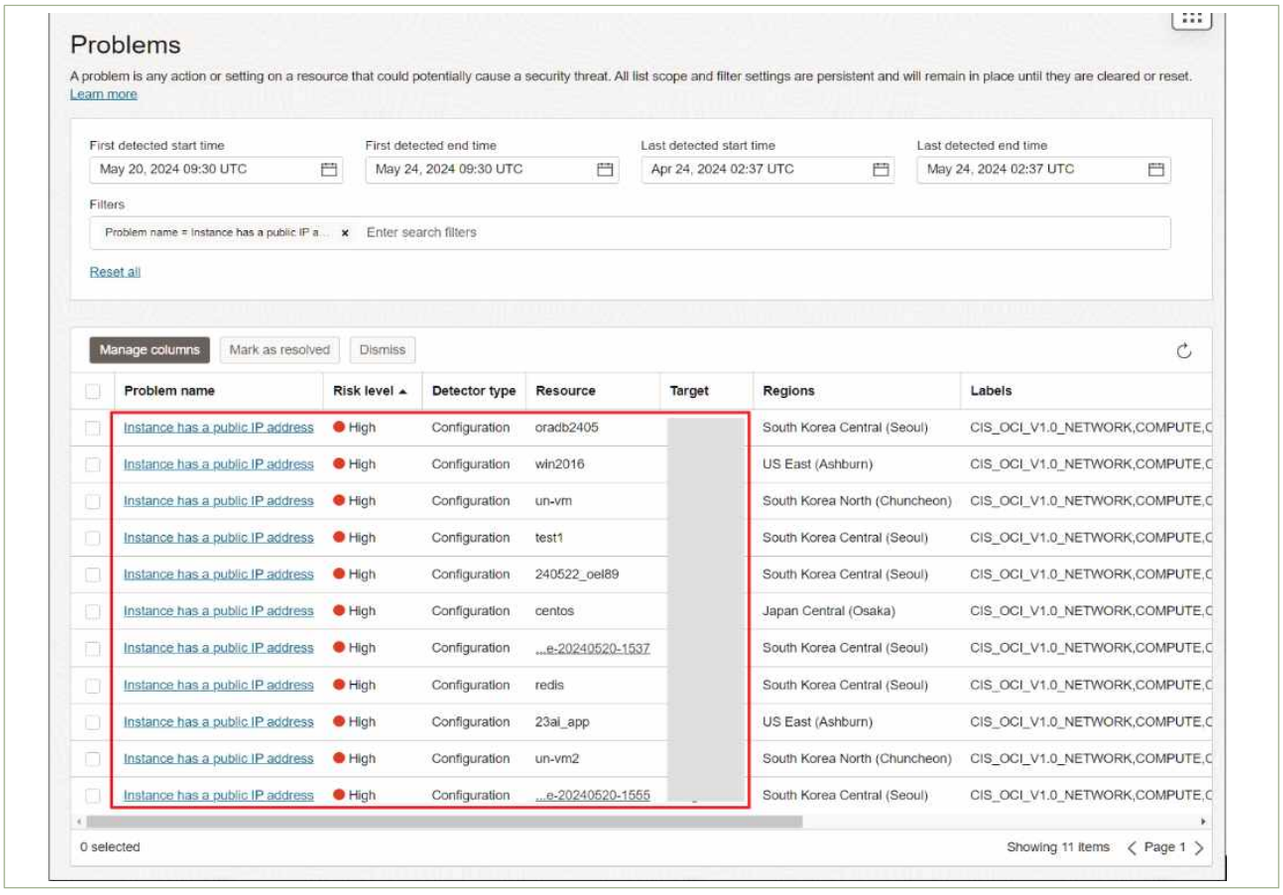


| 그림 1.4.3 | Public Subnet으로 구성된 인스턴스 탐지 룰

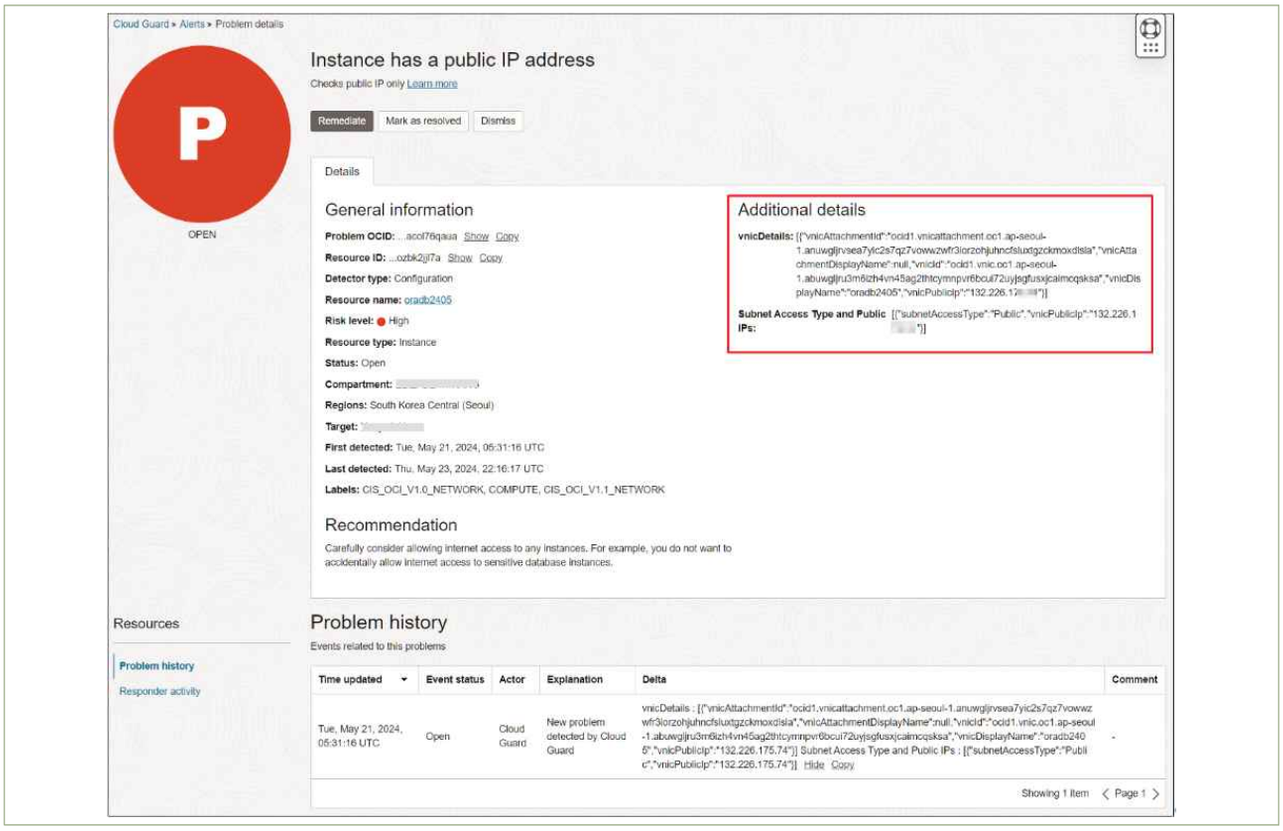
- 보안 및 구성 문제로 모니터링하고자 하는 전체 내용 중 조회 쿼리를 Instance has a public IP address로 지정 후 조회하면 공인 IP 할당된 전체 인스턴스(Instance) 조회됨



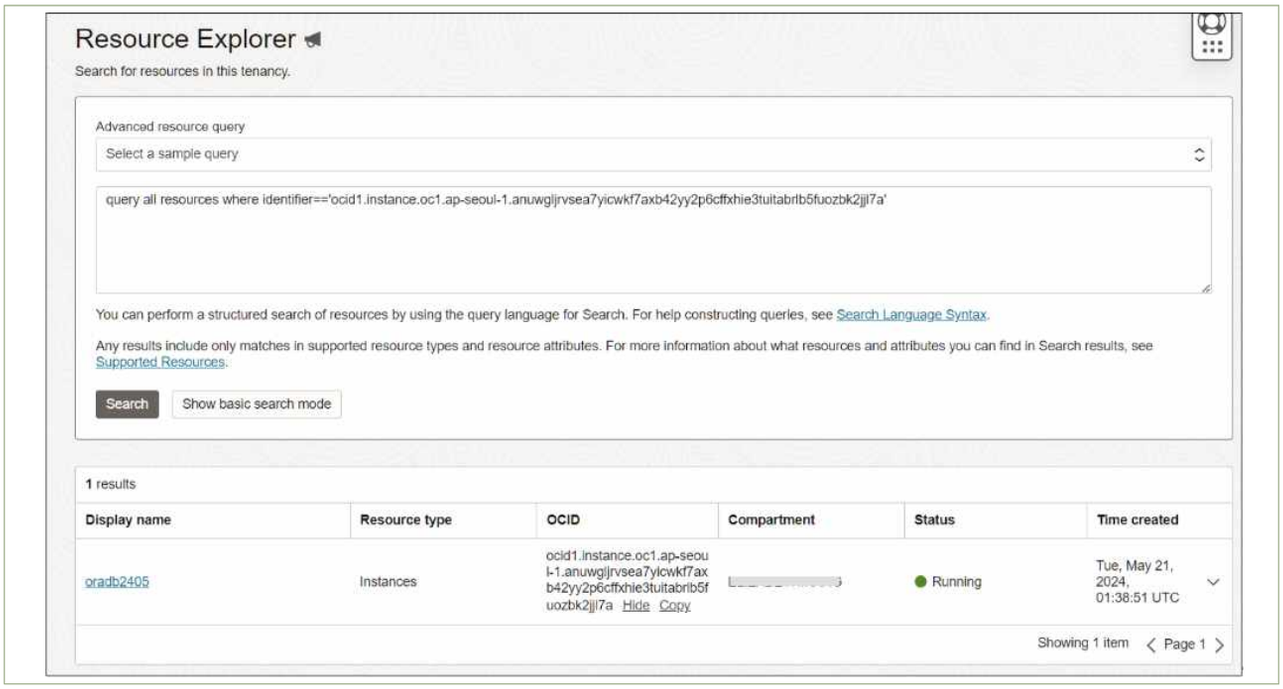
| 그림 1.4.3 | 조회 쿼리 지정



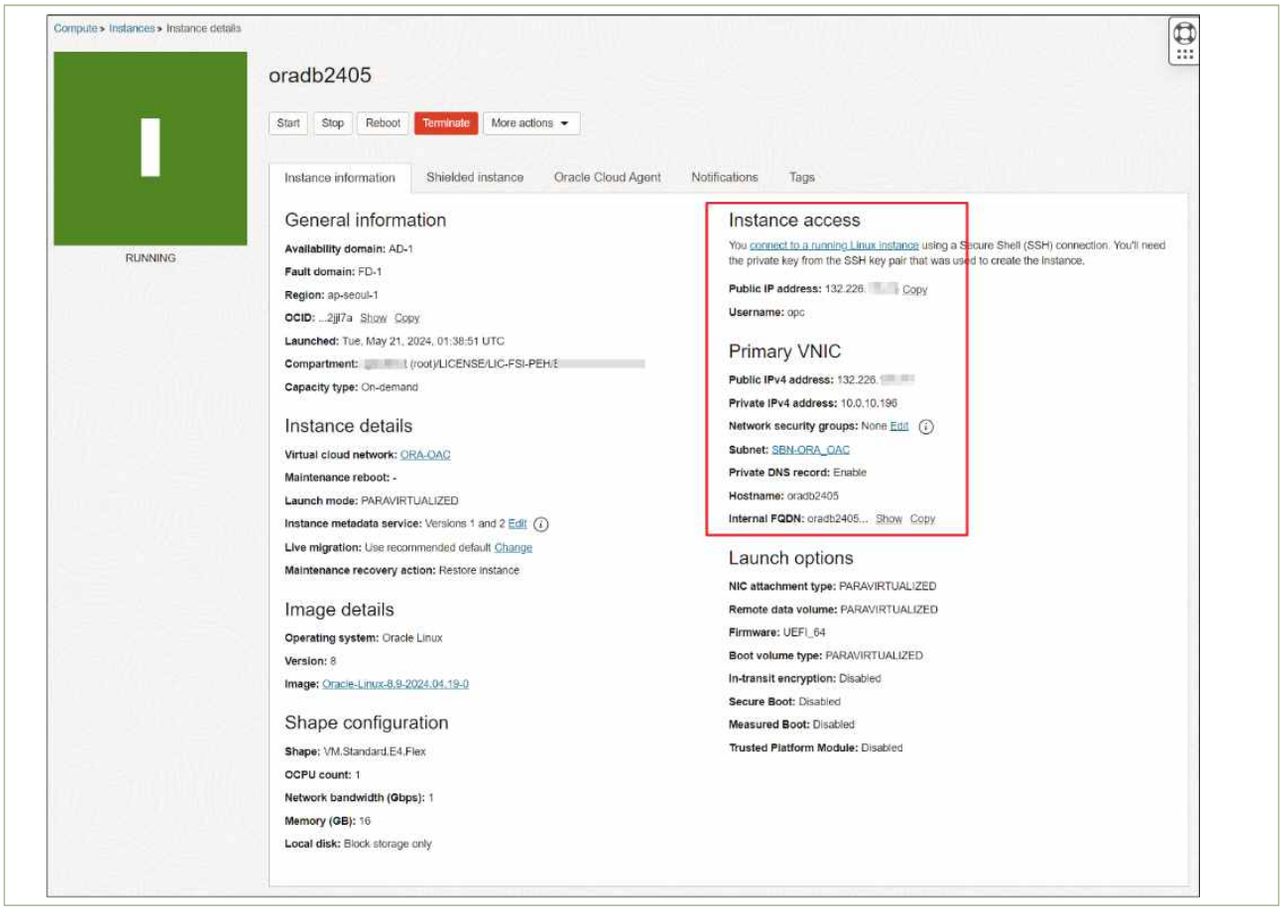
| 그림 1.4.4 | Public IP 조회 결과



| 그림 1.4.5 | 세부 정보



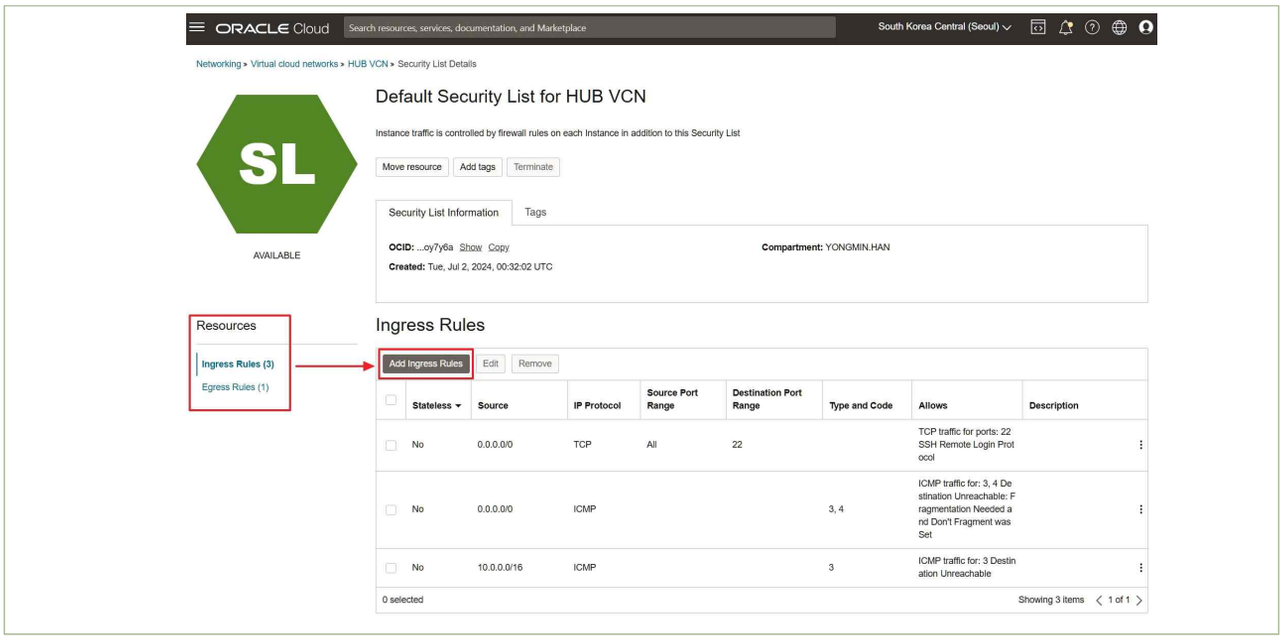
| 그림 1.4.6 | Resource Explorer 화면



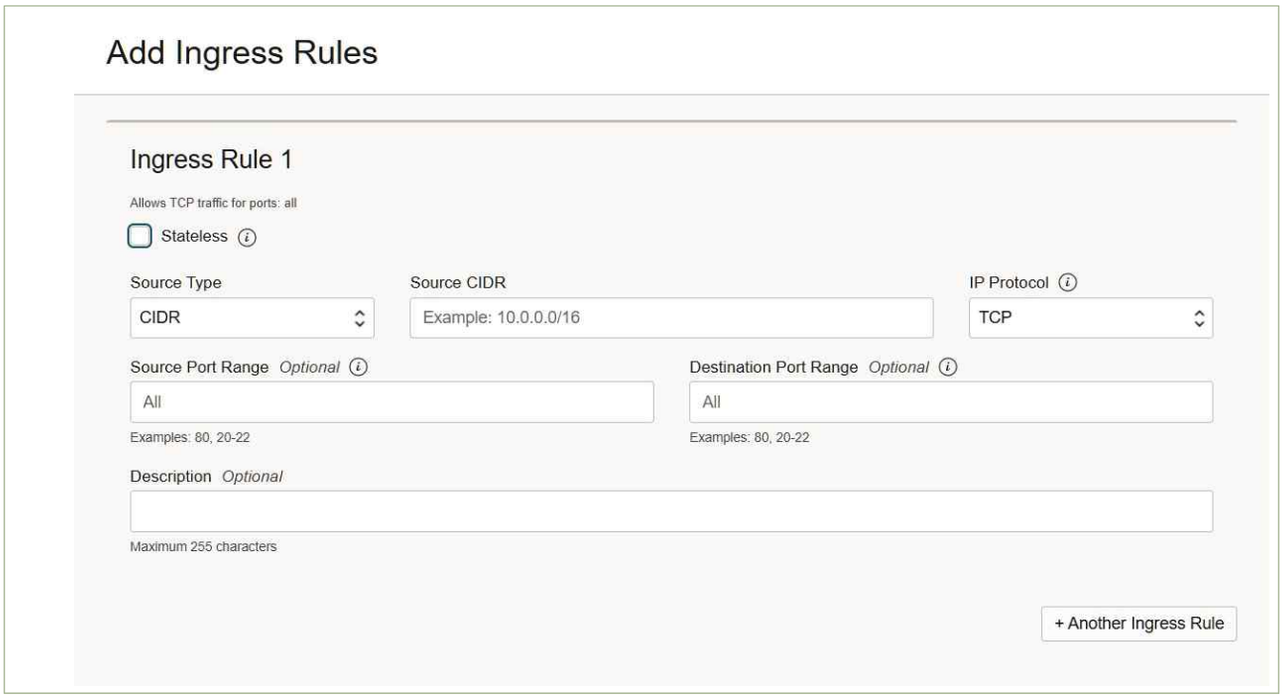
| 그림 1.4.7 | 인스턴스(Instance) 세부 정보

2) 접근 가능한 IP 또는 대역 설정

- OCI Security List를 통해 접근 가능한 IP 또는 IP 대역을 설정(Ingress Rules/Egress Rules IP/CIDR, Port, Protocol기반의 접근 정책 설정)



| 그림 1.4.8 | Ingress Rules 설정 화면



| 그림 1.4.9 | Ingress Rules 설정 화면

3) VPC 및 보안 그룹을 통한 내부 네트워크 대역 접근 설정
   - 2) 접근 가능한 IP 또는 IP 대역 설정 항목과 동일

4 참고 사항

- [VNIC 설정] https://cloud.oracle.com/compute/instances/create?region=ap-seoul-1
- [Public IP 보안정책]
  https://cloud.oracle.com/cloud-guard/detector_recipes?region=ap-seoul-1
- [보안모니터링] https://cloud.oracle.com/cloud-guard/problems?region=ap-seoul-1

1 기준

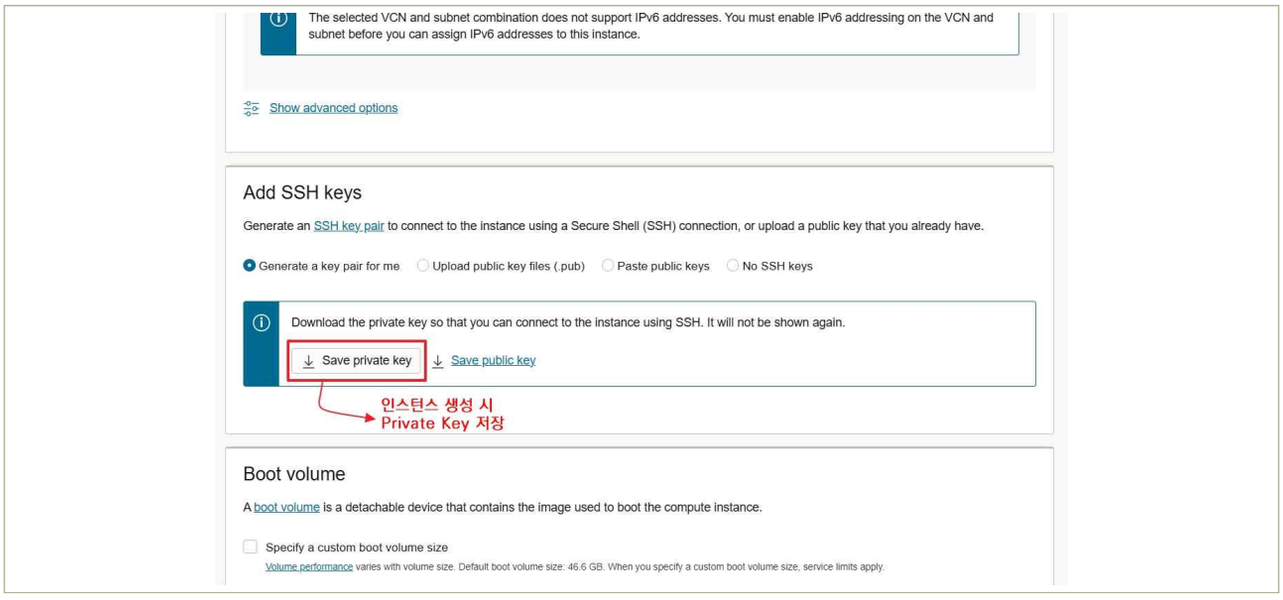
식별번호	기준	내용
1.5	**가상 자원 접속 시 보안 방안 수립**	이용자 가상 자원 접속 시 안전한 인증절차를 통해 접속하여야 한다.

2 설명

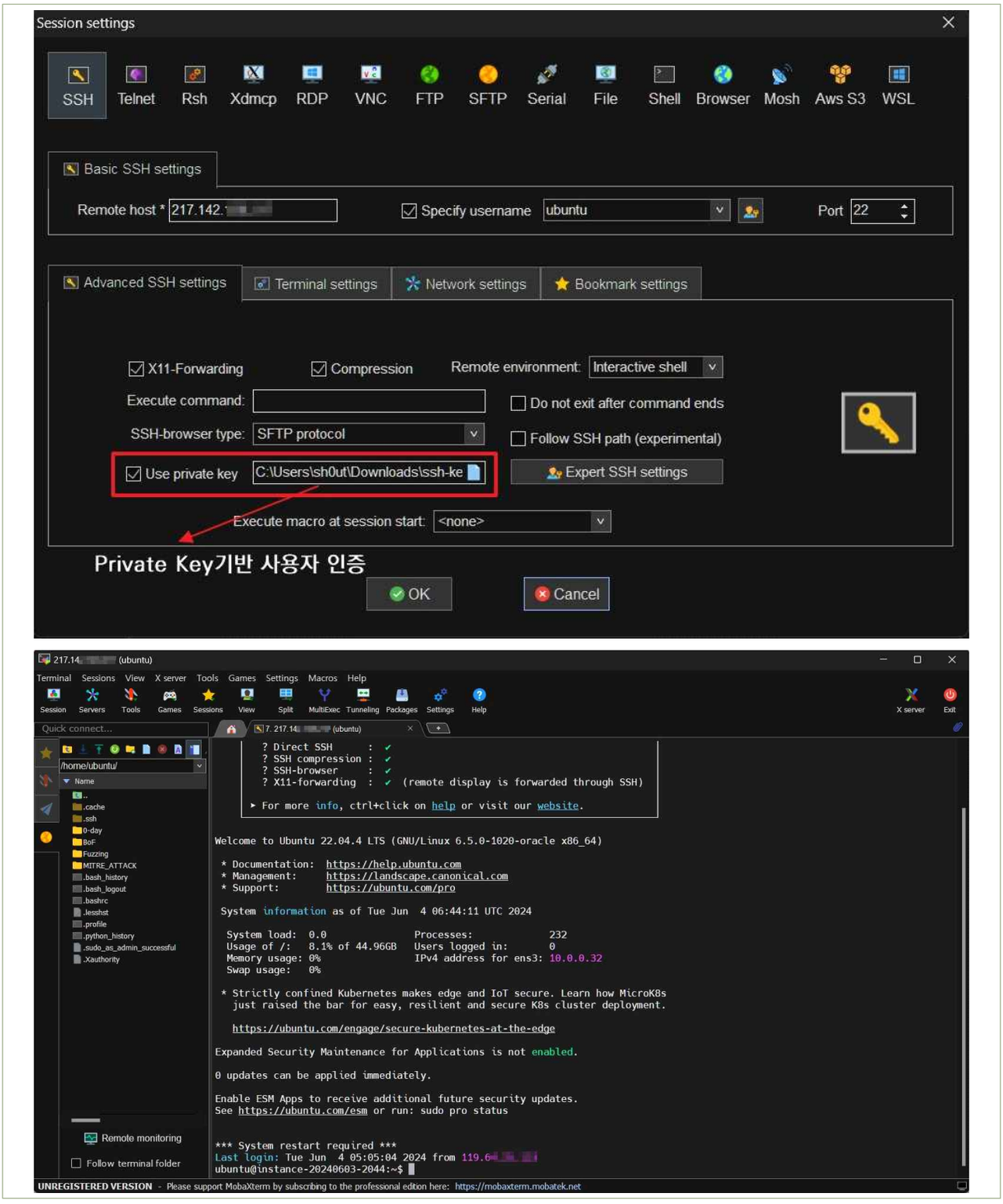
- 이용자의 가상 자원(인스턴스) 접속 시 안전한 방식을 통해 접근하여야 한다.
  1) SSH를 통한 접속 시 안전한 계정관리 수행(ex. ID/PW 기반이 아닌 Certificate 기반 인증 방식 적용)
  2) 클라우드 웹 콘솔에서 직접 실행 시 안전한 인증 방식 적용(해당 인스턴스를 호출할 수 있는 권한을 지닌 이용자인지 검증 등)

3 우수 사례

- (OCI 콘솔) '홈' → 'Compute' → 'Instances' → 'Create Instance'를 통해 인스턴스를 생성 할때, 제공되는 SSH Private Key를 저장하여 ID/비밀번호 방식이 아닌 Key 인증 방식을 통해 가상 자원에 접속 가능



| 그림 1.5.1 | 가상 자원 접속 시 Private Key 기반의 사용자 인증



| 그림 1.5.2 | 가상 자원 접속 시 Private Key 기반 사용자 인증

4 참고 사항

-

- [Compute] https://cloud.oracle.com/compute/instances/create?region=ap-seoul-1
- [IAM] https://www.oracle.com/kr/security/identity-management/

1 기준

식별번호	기준	내용
1.6	**이용자 가상 자원별 권한 설정**	이용자 직무 및 권한에 따른 가상 자원별 접근통제 방안(권한 설정 등)을 수립하여야 한다.

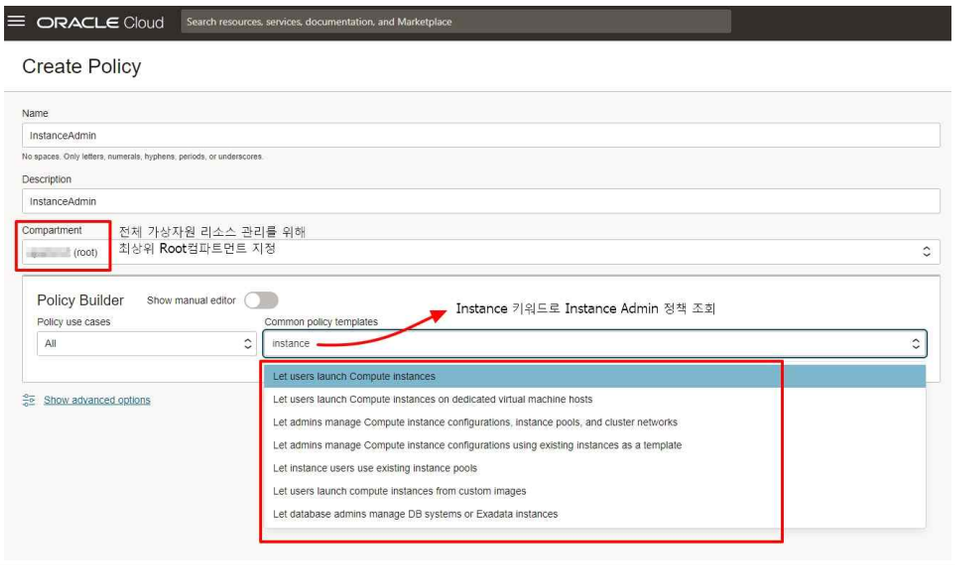
2 설명

- 이용자 직무 및 권한에 따른 가상 자원별 접근통제 방안(권한설정 등)을 수립하여야 한다.
  1) 가상 자원 종류별 접근통제 방안 수립(ex. IAM을 통한 접근권한 관리)
     - 모든 가상 자원에 접근 가능한 Role에 대해서는 최소 인원에 대해서만 부여

3 우수 사례

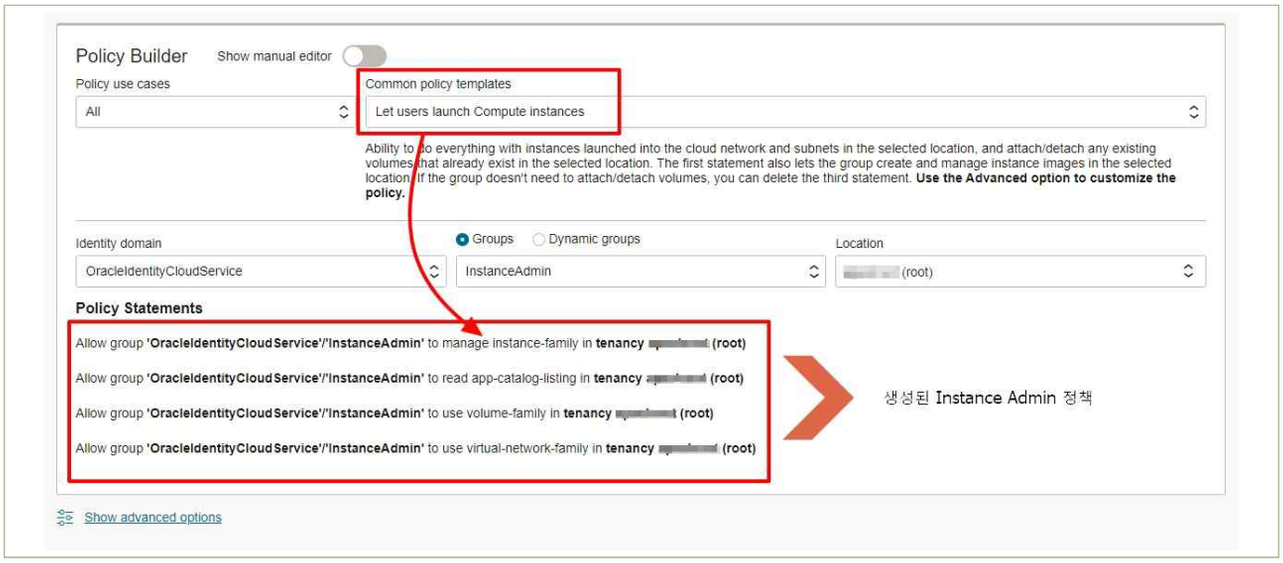
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' → 'Create Policy'에서 사용자 직무 및 권한에 따라 가상 자원별 접근 통제 방안을 수립

  모든 가상 자원에 접근 가능한 최상위 루트 컴파트먼트(Compartment)를 지정하고, Policy Builder → Instance로 검색하여 "Let admins manage Compute instance"가 포함된 정책을 선택



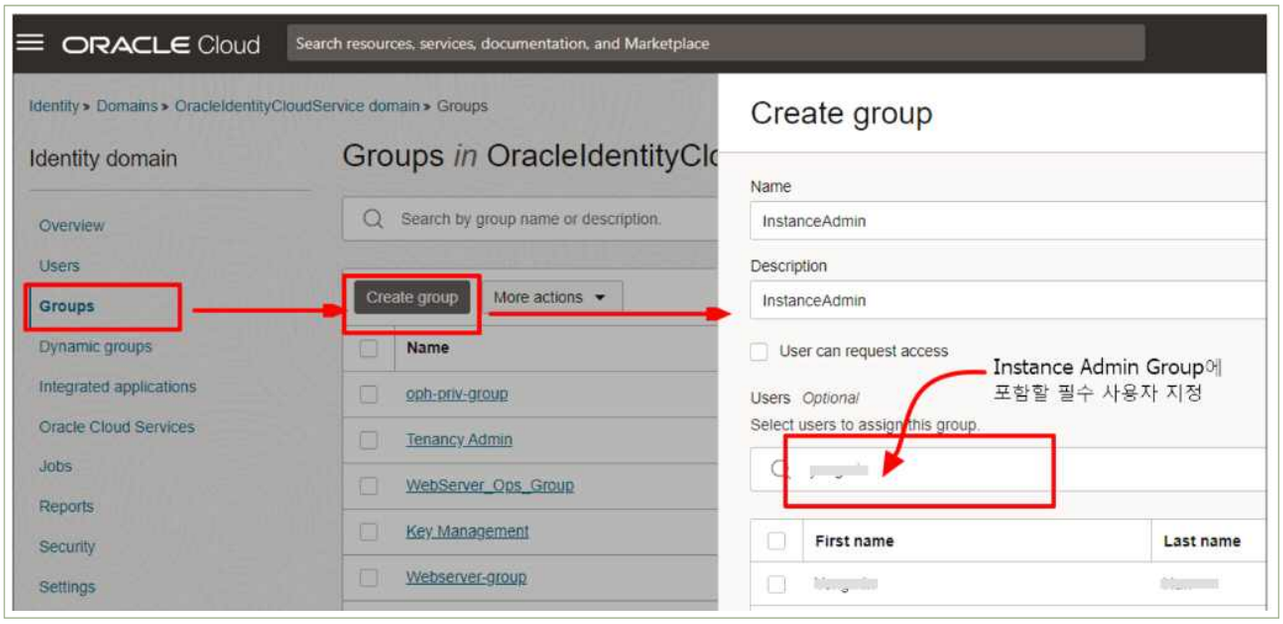
| 그림 1.6.1 | Create Policy

- Identity domain과 Groups, Location을 선택하면 Policy Builder가 생성한 정책을 확인할 수 있음
- 가상 자원별 접근 권한 설정을 위해 그룹별 사용자를 등록하면, 해당 그룹은 정책에 따라 가상 자원을 관리



| 그림 1.6.2 | Policy Builder

- 그룹 정책과 사용자 등록은 아래 내용을 참고하여 절차에 따라 생성



| 그림 1.6.3 | Create group

4 참고 사항

- [정책 및 권한할당]
  https://cloud.oracle.com/identity/domains/policies?region=ap-seoul-1
- [사용자 그룹] Identity 〉 Domain 〉 도메인(해당) 〉 Groups

1 기준

식별번호	기준	내용
1.7	**이용자 가상자원 내 악성코드 통제 방안 수립**	이용자 가상자원 내 악성코드 통제방안을 수립하여야 한다.

2 설명

- 이용자 가상자원 내 악성코드 통제방안을 수립하여야 한다.
  1) 이용자가 보유하고 있는 악성코드 통제방안 수립(백신 등)
  2) 클라우드 사업자가 악성코드 통제방안 제공(백신 등)
  3) 백신 등 설치가 불가능한 환경인 경우 그 수준에 준하는 악성코드 통제방안 수립

3 우수 사례

- 오라클 클라우드 마켓플레이스에서는 백신과 같은 악성코드 통제 솔루션을 제공하고 있지 않아 별도의 라이선스를 구매하여 가상 자원에 적용하여야 함

4 참고 사항

- N/A

2. 네트워크 관리

2.1. 업무 목적에 따른 네트워크 구성
2.2. 내부망 네트워크 보안 통제
2.3. 네트워크 보안 관제 수행
2.4. 공개용 웹 서버 네트워크 분리
2.5. 네트워크 사설 IP 주소 할당 및 관리
2.6. 네크워크(방화벽 등) 정책 주기적 검토

2 네트워크 관리

1 기준

식별번호	기준	내용
2.1	**업무 목적에 따른 네트워크 구성**	클라우드 환경 내 업무 목적에 따른 네트워크를 구성하여야 한다. * 개발, 운영 업무 등

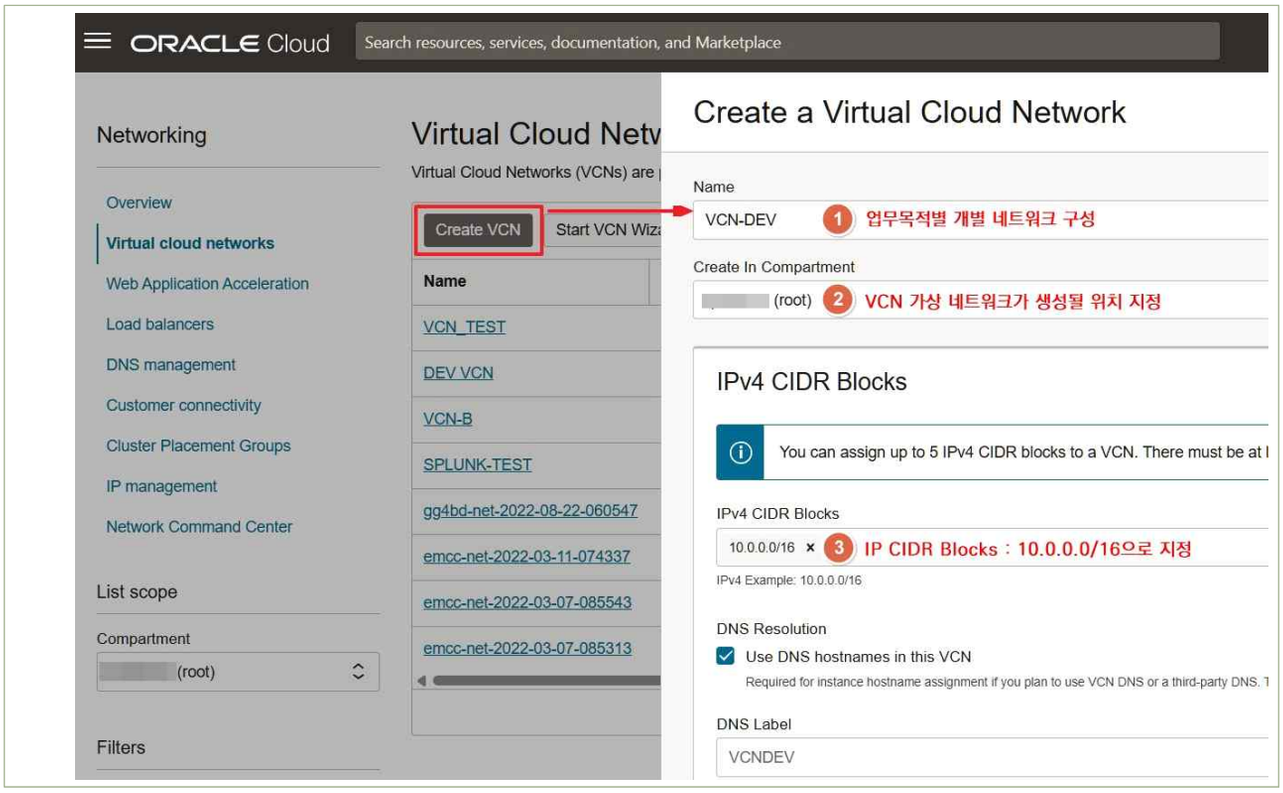
2 설명

- 클라우드 환경 내 업무 목적(개발, 운영, 업무 등)에 따른 네트워크 구성 및 네트워크간 접근 통제 방안을 수립하여야 한다.
  1) VPC 등 네트워크 관련 기능을 통한 네트워크 구성 및 통제
  2) 보안그룹(Security Group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)

3 우수 사례

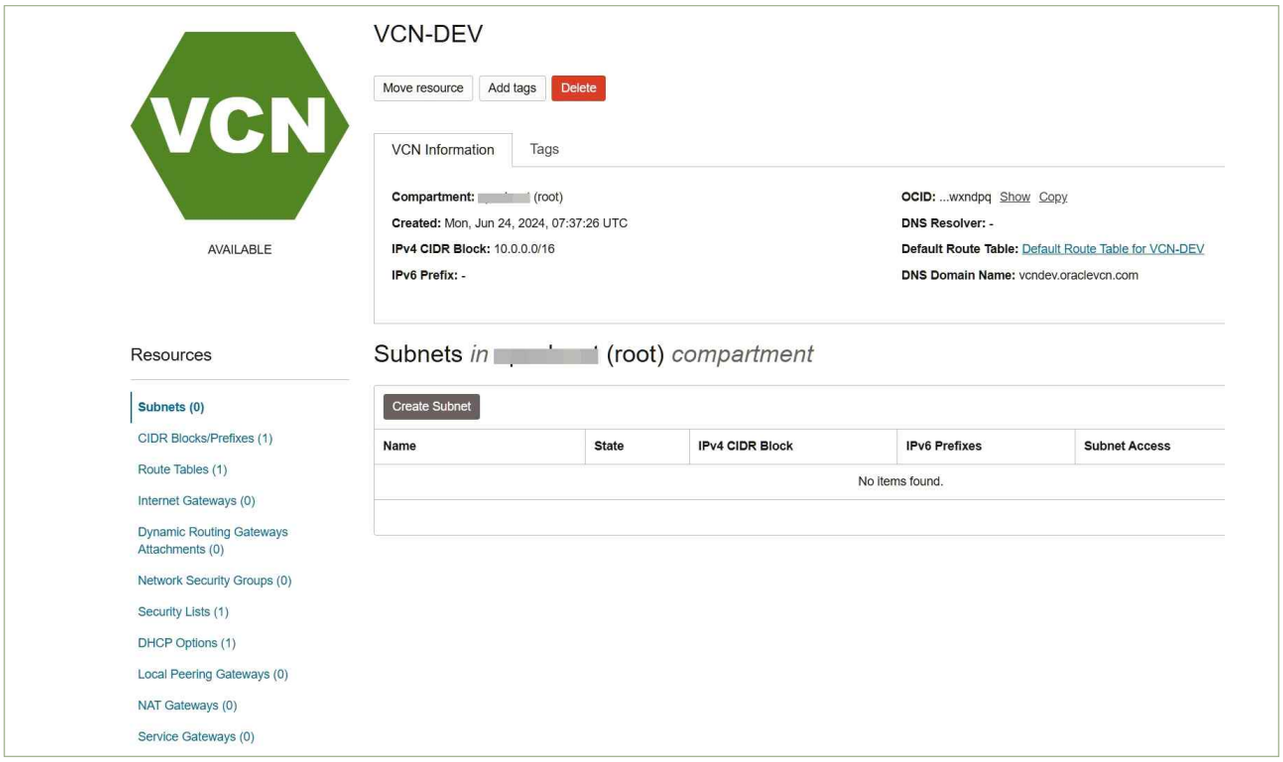
1) VPC 등 네트워크 관련 기능을 통한 네트워크 구성 및 통제

- (OCI 콘솔) '홈' → 'Networking' → 'Virtual cloud network' → 'Create VCN'에서 업무 목적에 맞는 VCN(Virtual Cloud Network)을 구성하고 통제 가능



| 그림 2.1.1 | VCN 네트워크 구성 화면

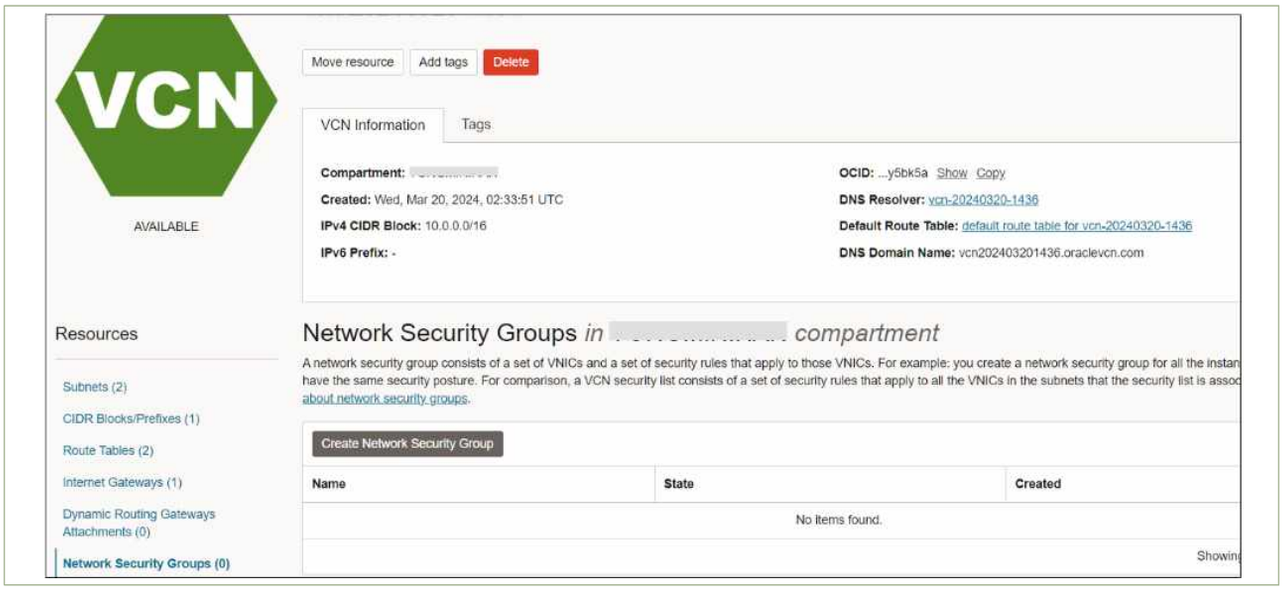
- 생성된 VCN(Virtual Cloud Network)과 네트워크 관련 리소스들



| 그림 2.1.2 | VCN 관련 리소스 화면

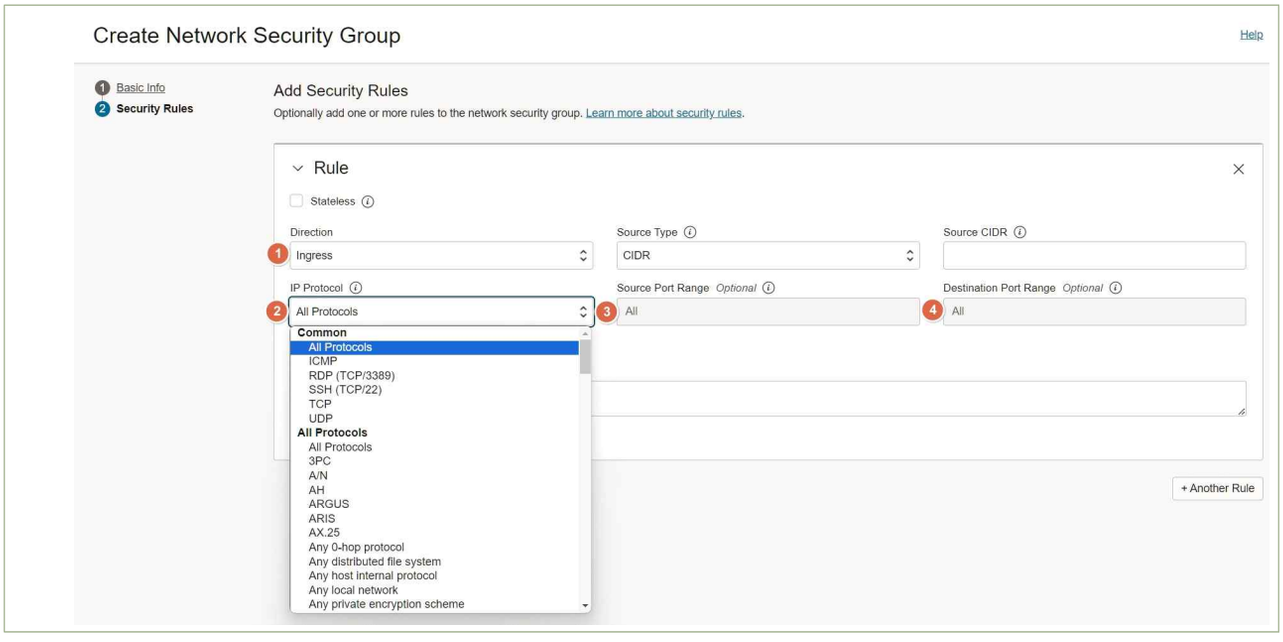
2) 보안 그룹(Security Group) 또는 NACL(Network ACL) 같은 기능을 활용해 네트워크를 구성하고 통제(인/아웃바운드 통제 등)

- (OCI 콘솔) '홈' → 'Networking' → 'Virtual cloud network' → 'Virtual Cloud Network Details' → 'Network Security Groups' → 'Create Network Security Group'



| 그림 2.1.3 | Network Security Group 생성

- Ingress(인바운드), Egress(아웃바운드), Source CIDR(IP 주소), IP Protocol을 지정하여 네트워크 구성 및 통제 방안 수립



| 그림 2.1.4 | Add Security Rules 설정

4 참고 사항

- [VCN 네트워크 구성] https://cloud.oracle.com/networking/vcns?region=ap-seoul-1

1 기준

식별번호	기준	내용
2.2	**내부망 네트워크 보안 통제**	클라우드 환경 내 내부망 구성 시 보안 통제 방안을 수립하고 적용하여야 한다.

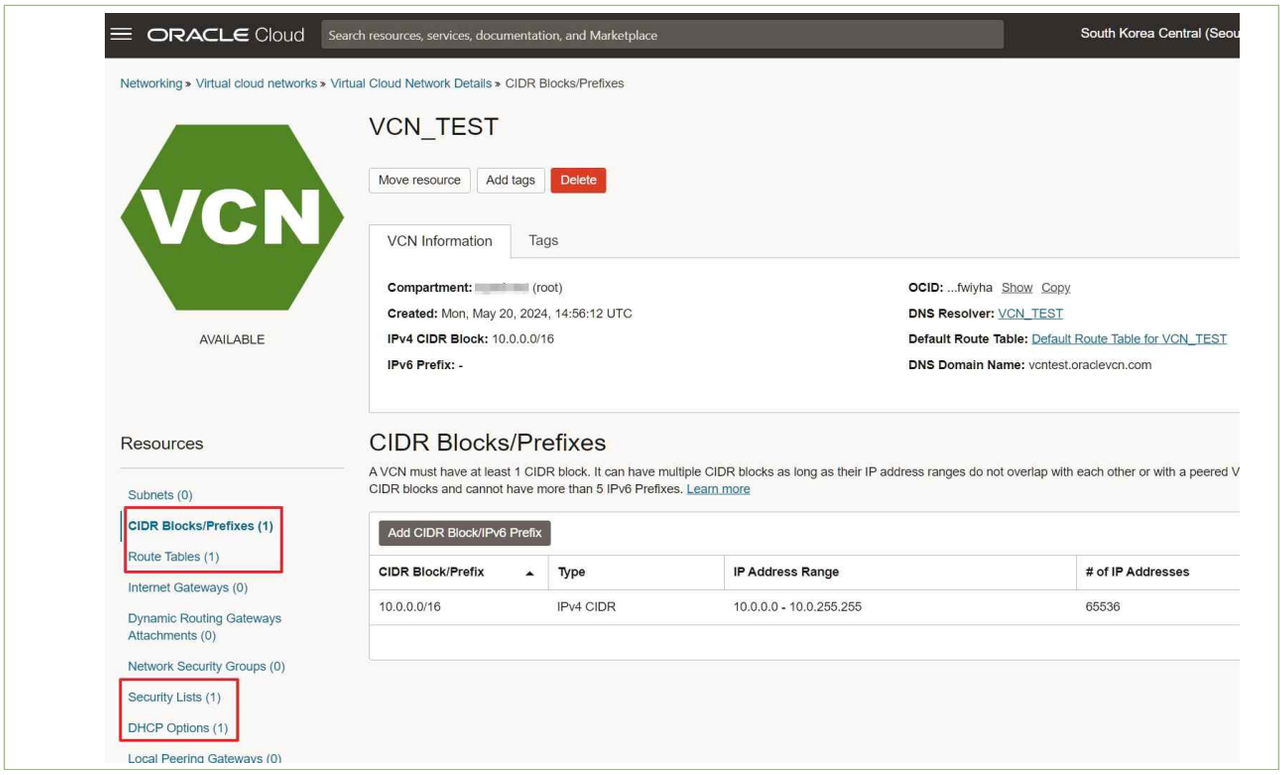
2 설명

- 클라우드 환경 내 내부망을 구성하는 경우 외부 침입, 비인가 접근 등으로 보호될 수 있도록 보안 통제 방안을 수립하고 적용하여 한다.
  1) VPC 등 네트워크 관련 기능을 통한 네트워크 접근 통제(인터넷망 등)
  2) 보안그룹(Security Group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성(인/아웃바운드 통제 등)
  3) 내부망으로 구현한 가상자원(서버, 데이터베이스 등)에 공인 IP 미할당
  4) 방화벽 서비스를 통한 IP 통제 등

3 우수 사례

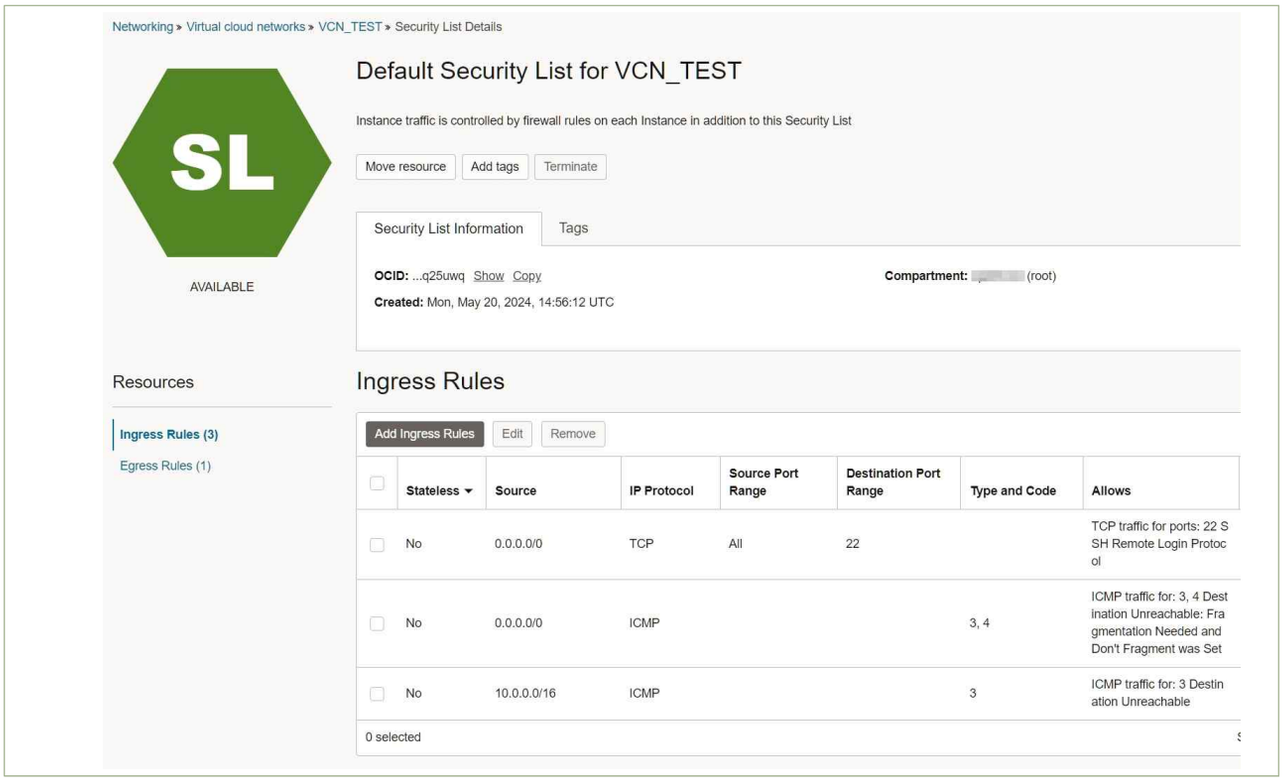
1) VPC 등 네트워크 관련 기능을 통한 네트워크 접근 통제(인터넷망 등)

- (OCI 콘솔) ‘홈’ → ‘Networking’ → ‘Virtual cloud network’ → ‘Create VCN’을 통해 VCN 생성 및 인터넷망 등 네트워크 접근 통제 기능 구현
  - ‘Create VCN’을 통해 VCN 생성할 때, Route Table 및 Security List, DHCP 등 네트워크 기본 구성 요소로 구성 (수동 모드로 VCN을 구성하면 Internet Gateway는 구성되지 않음)
  - ‘Create VCN’(수동모드)로 생성한 VCN 네트워크 구성 설정



| 그림 2.2.1 | VCN 구성 설정

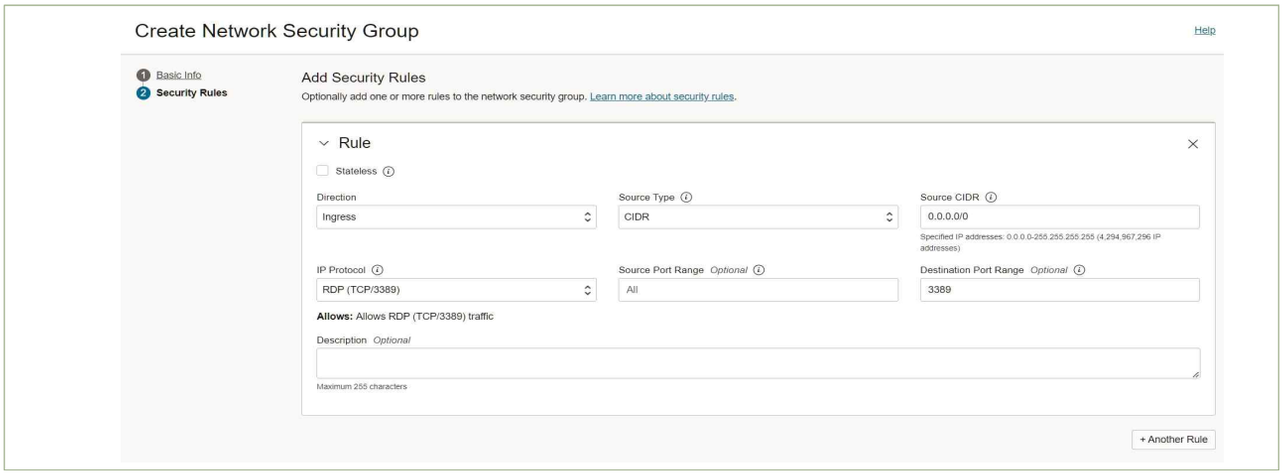
- 네트워크 접근 제어를 위해 보안 목록(Security List)의 구성 상태 확인 및 설정



| 그림 2.2.2 | Security List 구성

2) 보안 그룹(Security Group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성(인/아웃바운드 통제 등)

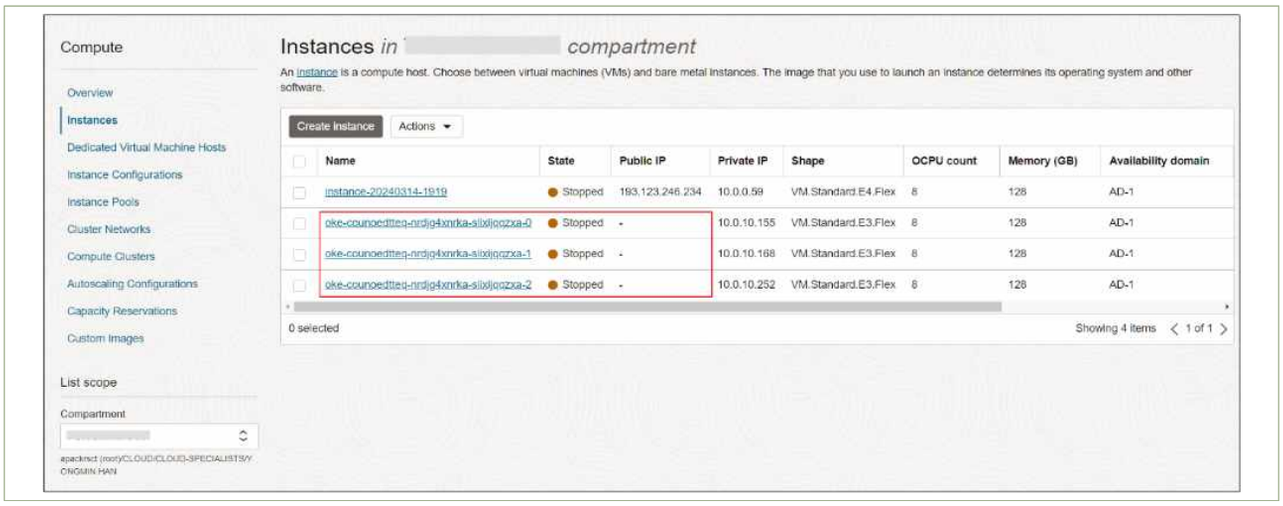
- (OCI 콘솔) '홈' → 'Networking' → 'Virtual cloud network'에서 네트워크 보안 그룹(Network Security Group)이 구성된 VCN을 선택하여 보안 규칙(Security Rules) 설정
  1) 네트워크 보안 그룹(Network Security Group)를 통한 네트워크 분리
     - 퍼블릭 서브넷(Public Subnet)에 대한 인바운드(Ingress) 규칙을 설정하여 HTTP, HTTPS 트래픽만 허용
     - 프라이빗 서브넷(Private Subnet)에 대한 인바운드 규칙을 설정하여 SSH, RDP 트래픽만 허용



| 그림 2.2.3 | Network Security Group 구성

3) 내부망으로 구현된 가상 자원(서버, 데이터베이스 등)에는 공인 IP 미할당

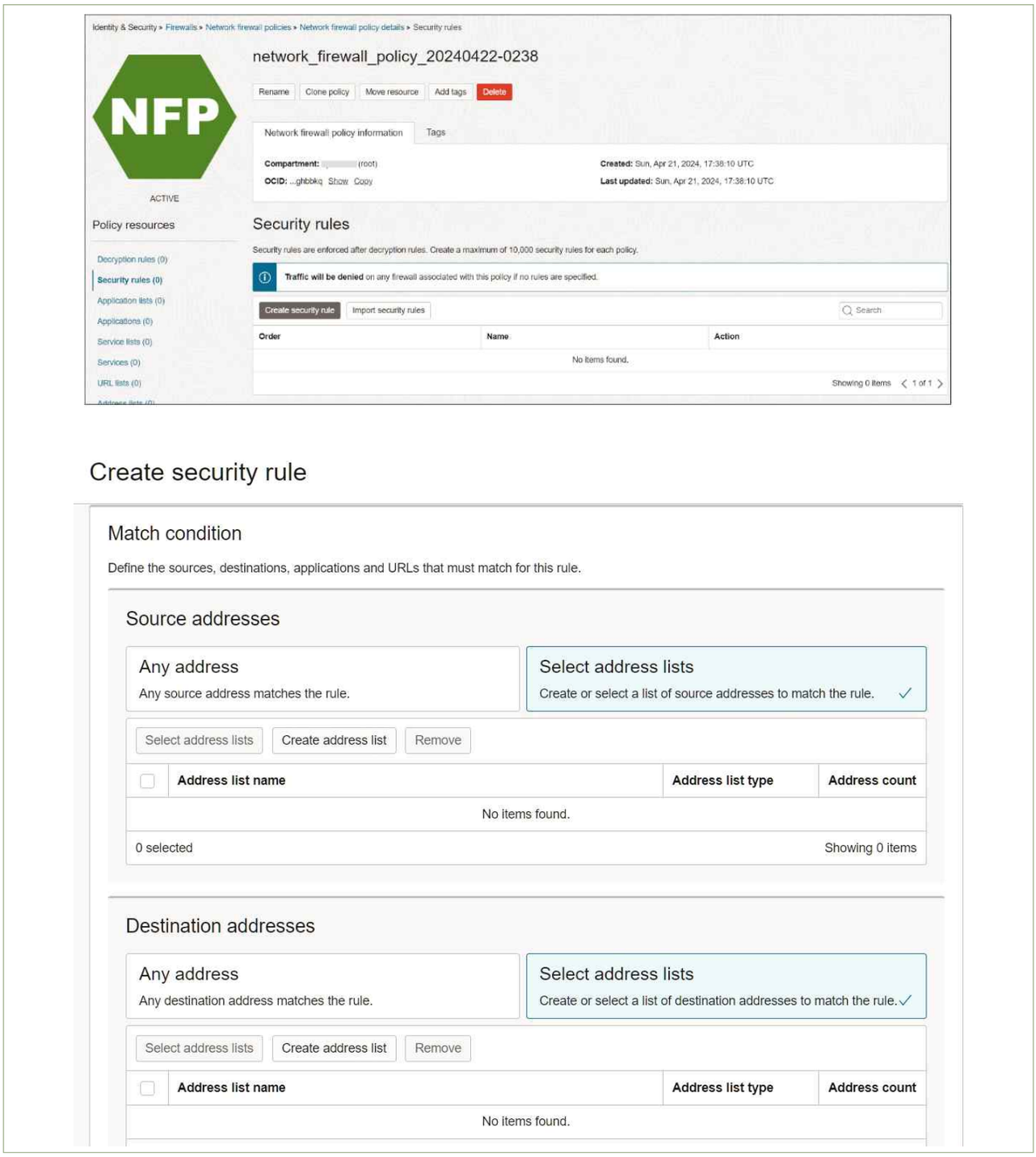
- (OCI 콘솔) '홈' → 'Compute' → 'Instances'에서 내부망으로 구현된 컴퓨팅 인스턴스에 공인 IP 미할당



| 그림 2.2.4 | 내부 Compute Instance 공인 IP 부여 현황 확인

4) 방화벽 서비스를 활용한 IP 통제 등

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Firewalls' → 'Network Firewalls' → 'Network Firewall Policies' → 'Create network firewall policy' → 'Security rules' → Create Security rule'에서 Source addresses/Destination addresses에서 통제하고자 하는 IP 목록을 구성



| 그림 2.2.5 | 네트워크 방화벽(Network Firewall)을 활용한 IP 통제 정책 구성

4 참고 사항

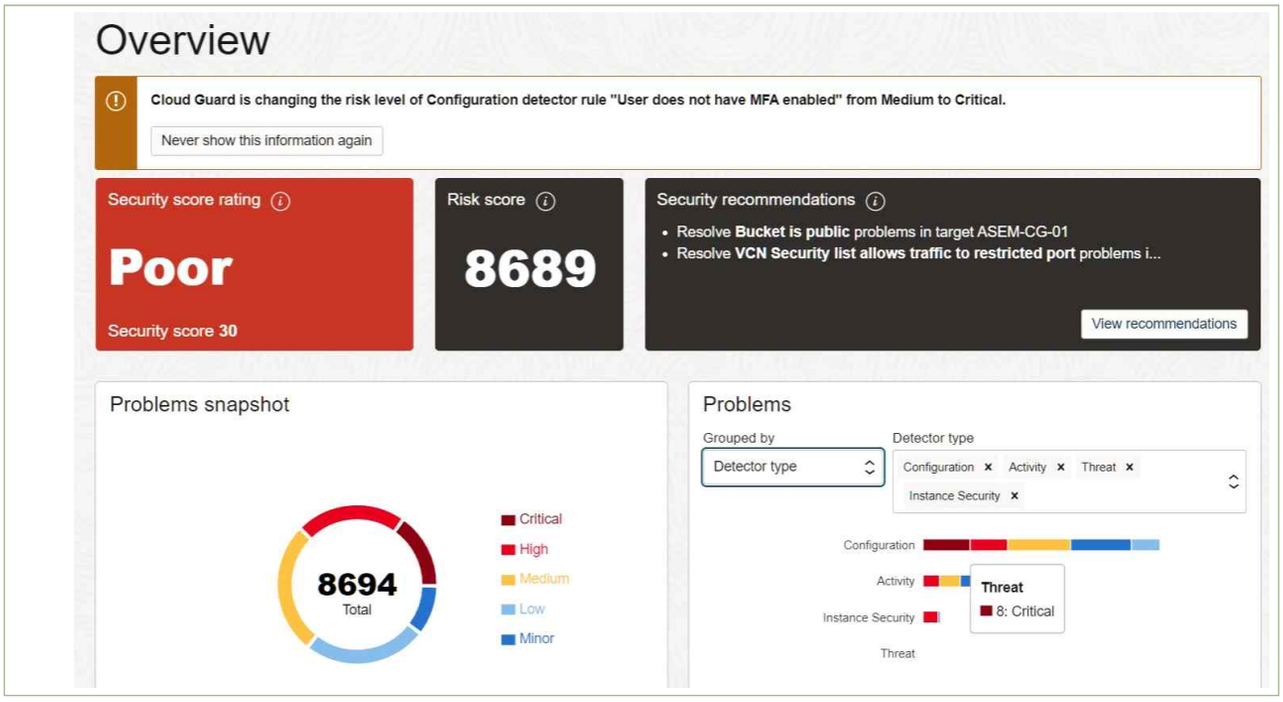
- [네트워크 구성] https://cloud.oracle.com/networking/vcns?region=ap-seoul-1
- 보안 통제를 구성할 VCN(Virtual Cloud Network) 선택 → Network Security Groups → Create Network Security Group → Basic Information 작성 → Add Security Rules 작성

1 기준

식별번호	기준	내용
2.3	**네트워크 보안 관제 수행**	클라우드 환경 내 금융회사 가상자원을 보호하기 위한 네트워크 보안 관제를 수행하여야 한다.

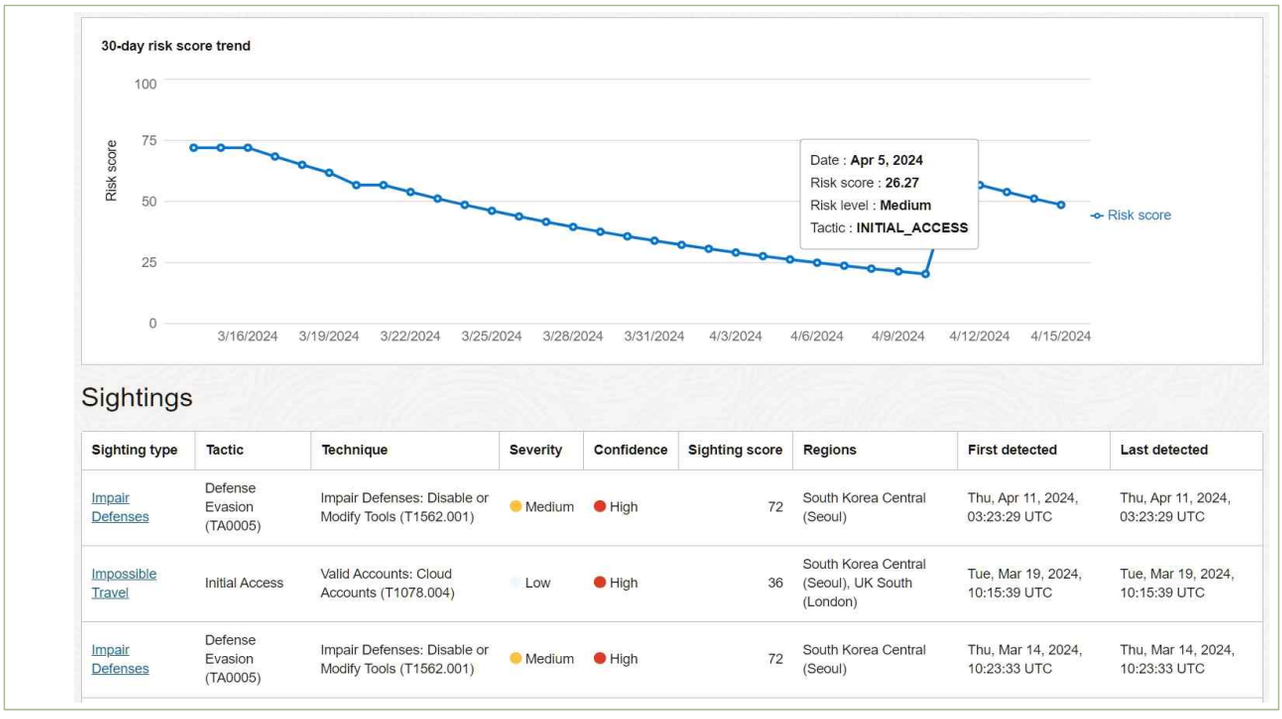
2 설명

- 클라우드 환경 내 가상자원을 보호하기 위해 네트워크 보안 관제를 수행하여야 한다.
  1) 금융회사 보안 관제 서비스와 연동하여 관제 수행(클라우드 내 발생하는 네트워크 트래픽 연동 등을 활용) → 금융보안과 오라클은 네트워크 트래픽 연동을 위한 테스트를 완료하였으며, 추후 관련 매뉴얼 업데이트 예정
  2) 클라우드 서비스 제공자가 제공하는 가상자원 보호를 위한 네트워크 보안관제 및 유사 기능(DDoS, WAF 등) 활용
  3) 클라우드 서비스 제공자가 제공하는 가상자원 보호를 위한 네트워크 보안관제 및 유사 기능 활용
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Cloud Guard' → 'Overview'



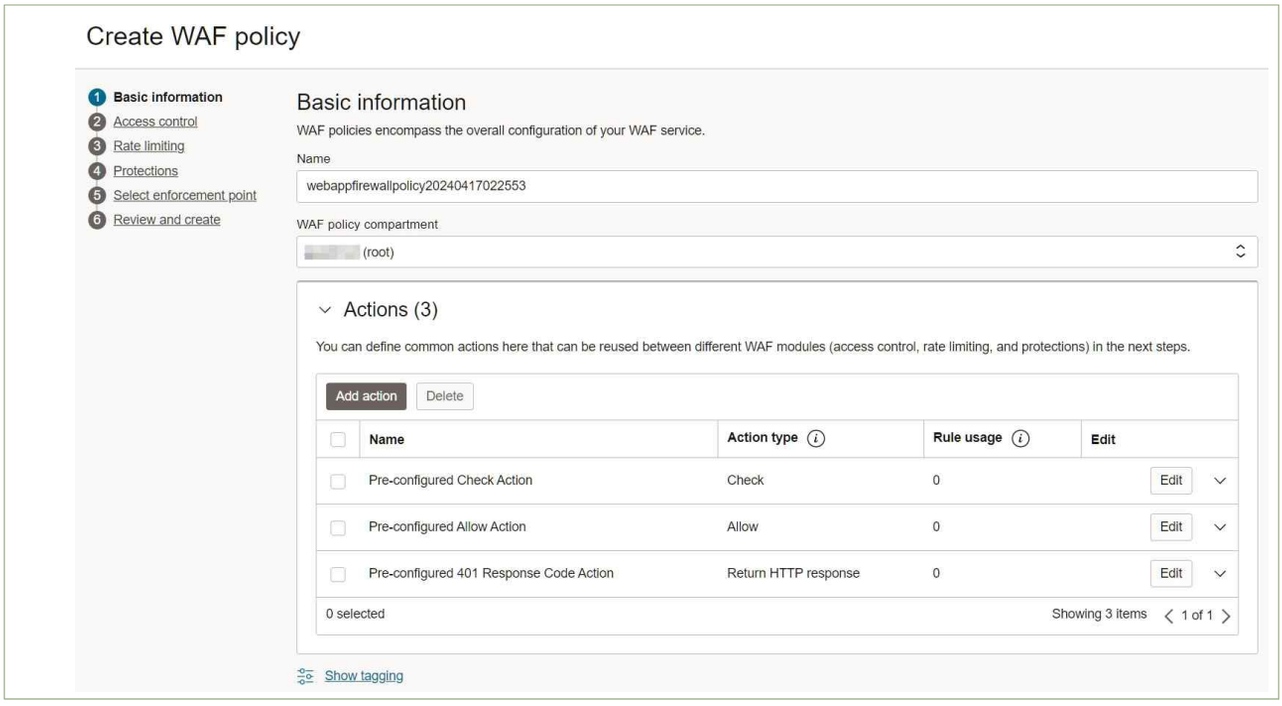
| 그림 2.3.1 | Cloud Guard를 통한 통합 보안 모니터링

- MITRE ATT&CK Framework 기반으로 다양한 보안 위협을 모니터링하고 위협 정보를 제공



| 그림 2.3.2 | 30-day risk score trend

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Web Application Firewall' → 'Create WAF policy'에서 OWASP Top 10에 기반한 WAF 보안 및 탐지 정책을 설정

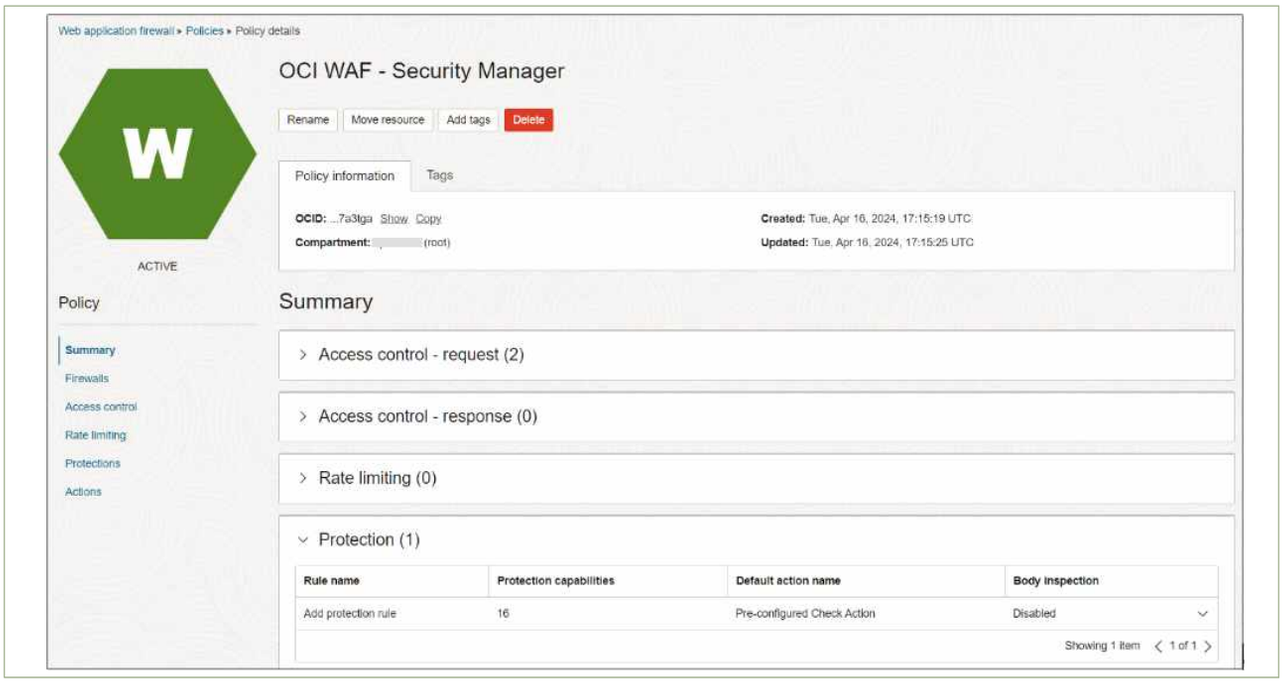


| 그림 2.3.3 | WAF 정책 설정

- OWASP Top 10에 기반한 웹 공격 차단 정책을 활성화
- 접근 제어(Access Control) 및 동작(Action) 설정을 활성화

Key	Name	Description	Collaborative	Tags
942270	SQL Injection (SQLi) Common SQLi attacks for various dbs	SQL Injection (SQLi) Attempt: Common attacks against msql, oracle, and other dbs detection	No	vendor-oracle, db-oracle, db-mysql, vendor-microsoft, db-mssql, db-postgresql, rdbms, PCI, Request-Body-Inspection, Recommended, OWASP-A1-2017, OWASP-A3-2021, CAPEC-1000, CAPEC-152, CAPEC-248, CAPEC-66, Command Injection, SQL Injection (SQLi), CVE-2023-0875
9420000	SQL Injection (SQLi) Collaborative Group - SQLi Filters Categories	SQL Injection (SQLi) Attempt: SQLi Filters via libinjection - Detect Database names - PHPIDS - Converted SQLI Filters.	Yes	db-mysql, db-mssql, db-mongodb, db-postgresql, db-oracle, db-sqlite, rdbms, nosql, Request-Body-Inspection, PCI, Collaborative, Recommended, OWASP-A1-2017, OWASP-A3-2021, Command Injection, SQL Injection (SQLi), CVE-2023-0630, CVE-2023-0875, CVE-2023-28661, CVE-2023-23488, CVE-2023-23489, CVE-2023-23490, CVE-2023-26325, CVE-2023-28659, CVE-2023-28660, CVE-2023-28662, CVE-2023-28663
	Cross-Site Scripting (XSS)	Cross-Site Scripting (XSS) Attempt: XSS Filters -		HTTP, PCI, Request-Body-Inspection, Recommended,

| 그림 2.3.4 | 웹 공격 차단 정책



| 그림 2.3.5 | OCI WAF 설정 완료

4 참고 사항

- [Cloud Guard] https://cloud.oracle.com/cloud-guard/overview?region=ap-seoul-1
- [Web Firewall] https://cloud.oracle.com/waf/policies?region=ap-seoul-1

1 기준

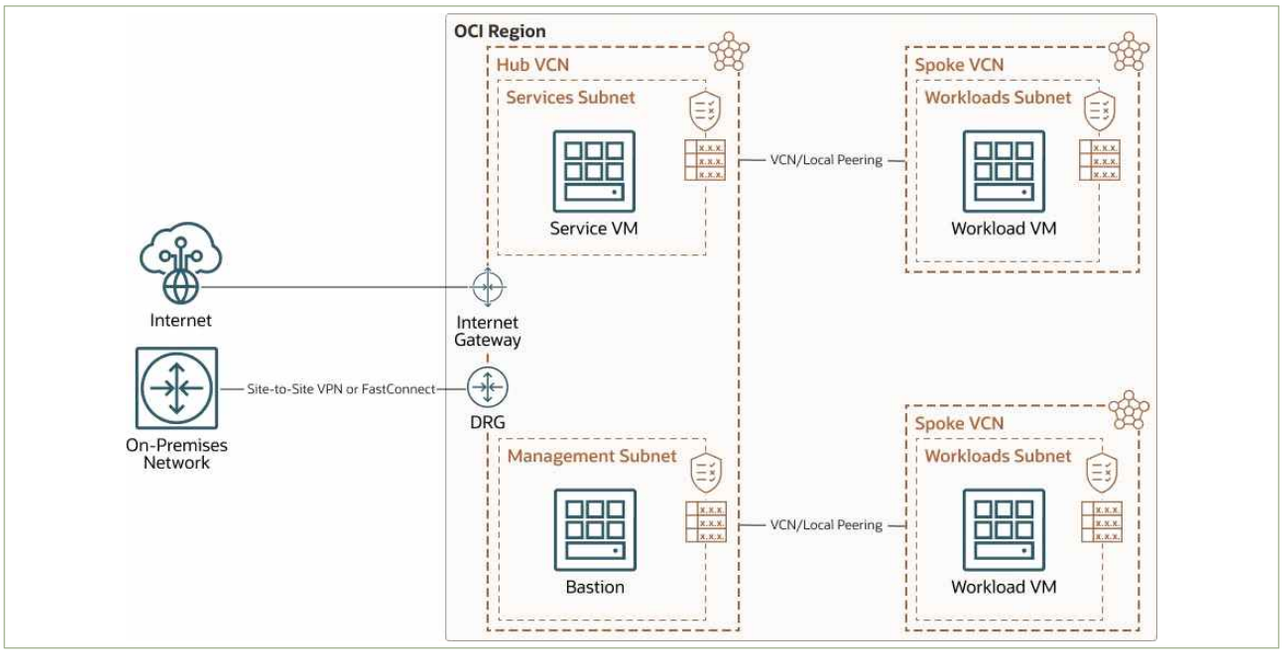
식별번호	기준	내용
2.4	**공개용 웹 서버 네트워크 분리**	클라우드 환경을 통한 공개용 웹 서버 구현 시 내부통신망과 분리하여 내부통신망과 외부통신망 사이 별도의 독립된 통신망("이하 DMZ")을 구현하고 안전하게 보호하여야 한다.

2 설명

- 클라우드 환경을 통한 공개용 웹 서버의 경우 내부통신망과 분리하여 내부통신망과 외부통신망 사이 별도의 독립된 통신망에 구현하고 접근통제를 수행하여야 한다.
  1) VPC 등 네트워크 분리 기능을 통한 DMZ 망 구축 후 공개용 웹 서버 구현
  2) 공개용 웹 서버 직접 접근 시 통제(ACL 등)에 의한 중요단말기 등에서 접근하도록 관리

3 우수 사례

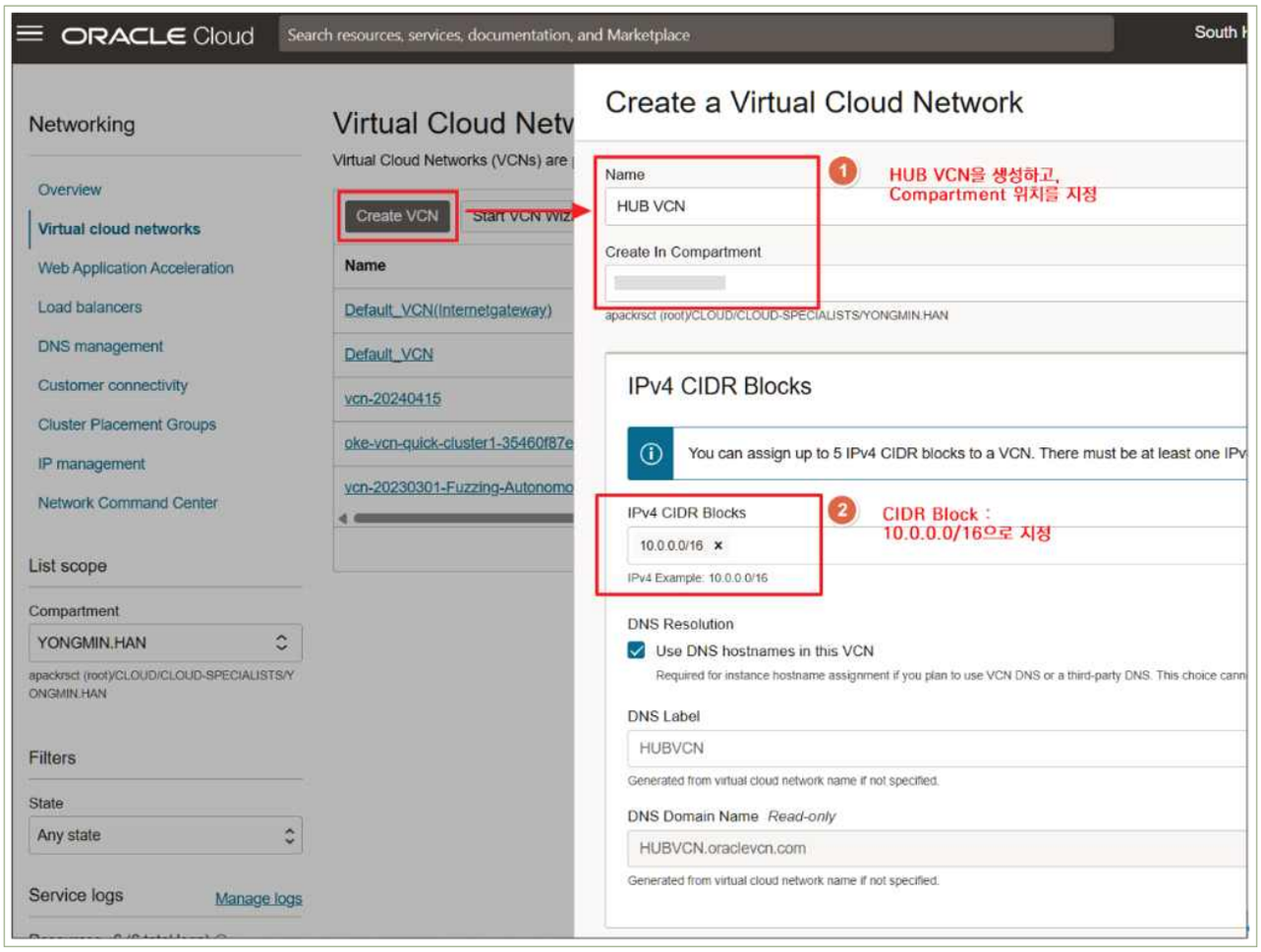
- (OCI 콘솔) '홈' → 'Networking' → 'Virtual cloud network'에서 허브-스포크(Hub-spoke) 아키텍처를 기반으로 웹 서버와 배스천(Bastion) 호스트를 구성



| 그림 2.4.1 | Hub-spoke architecture

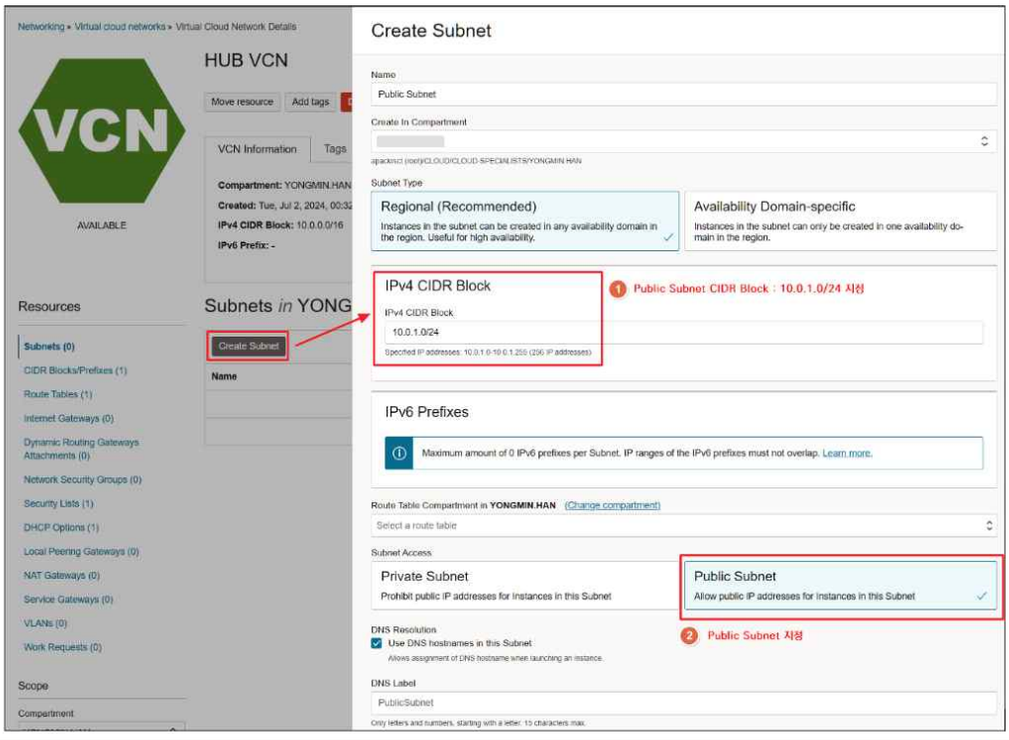
1) VCN 및 Subnet 구성(Hub-spoke 아키텍처)

- [Hub VCN 생성]
  - CIDR Block : 10.0.0.0/16
  - Subnets
    - Public Subnet(DMZ) : 10.0.1.0/24
    - Private Subnet : 10.0.2.0/24
- [Spoke VCN 생성]
  - CIDR Block : 10.1.0.0/16
  - Subnets
    - Public Subnet : 10.1.1.0/24
    - Private Subnet : 10.1.2.0/24
    - Hub VCN 생성



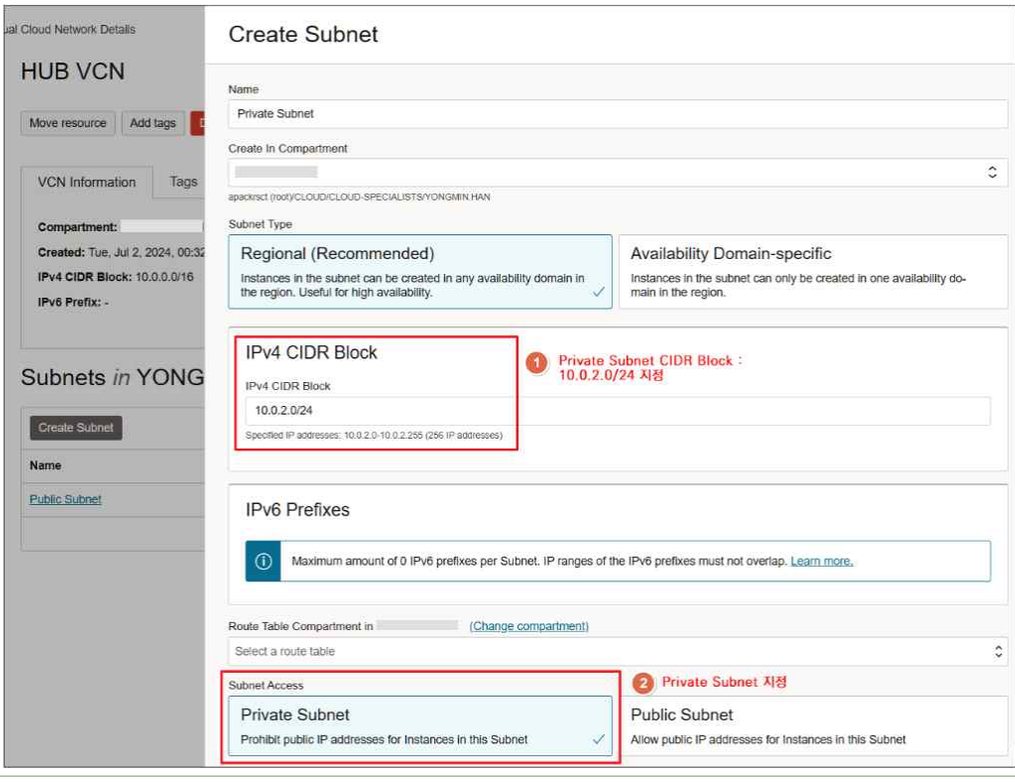
| 그림 2.4.2 | VCN 설정 화면

- Hub VCN Subnet 생성(Public)

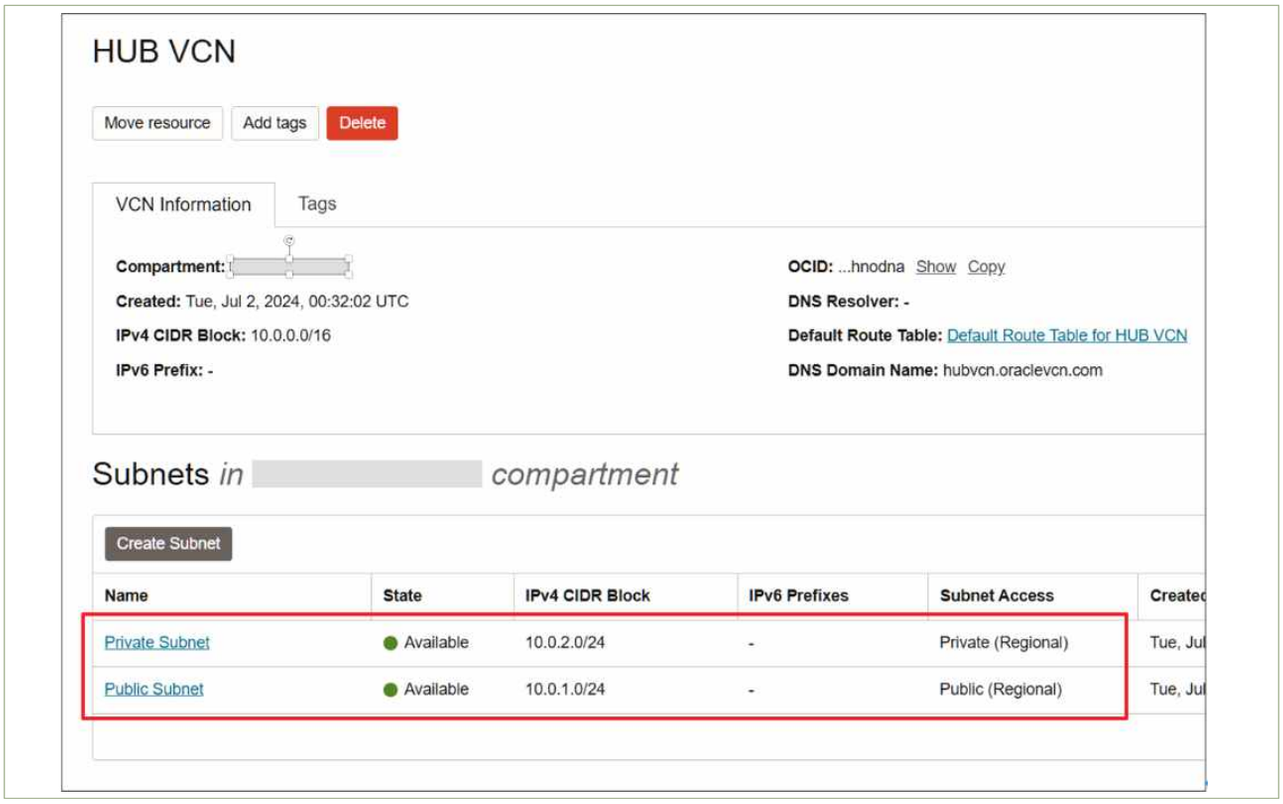


| 그림 2.4.3 | Create Subnet(Public)

- Hub VCN Subnet 생성(Private)

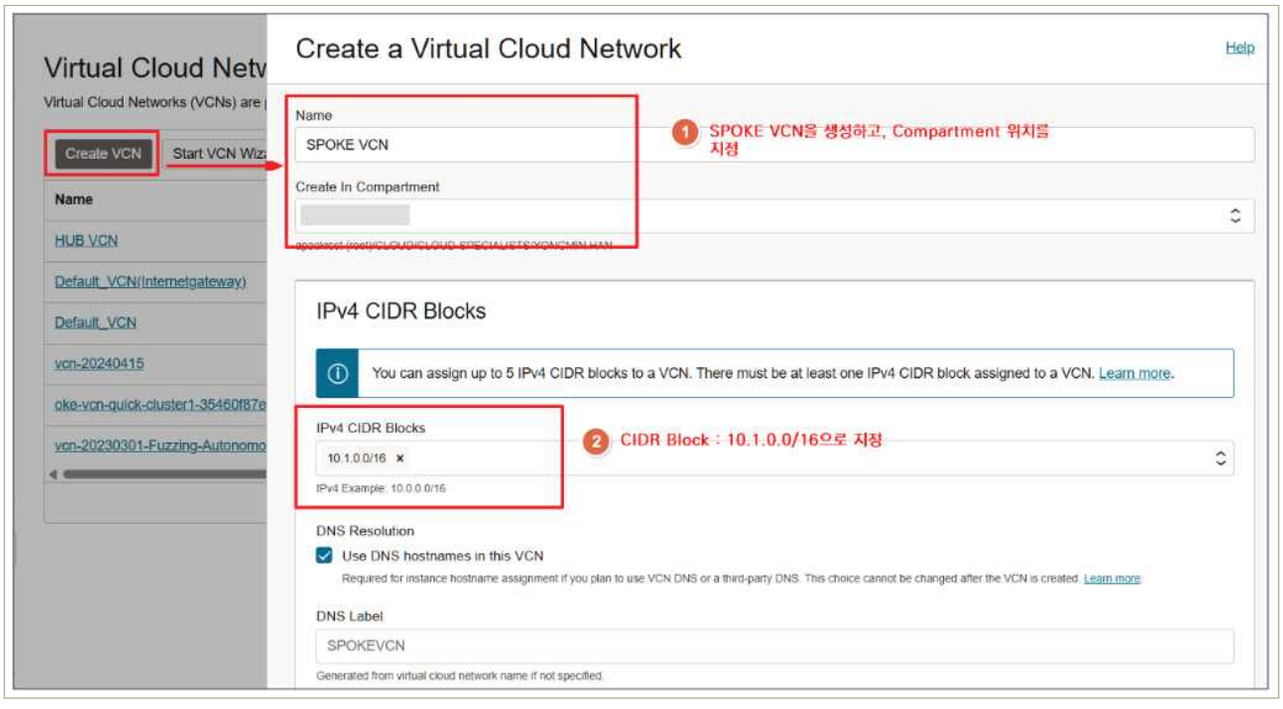


| 그림 2.4.4 | Create Subnet(Private)



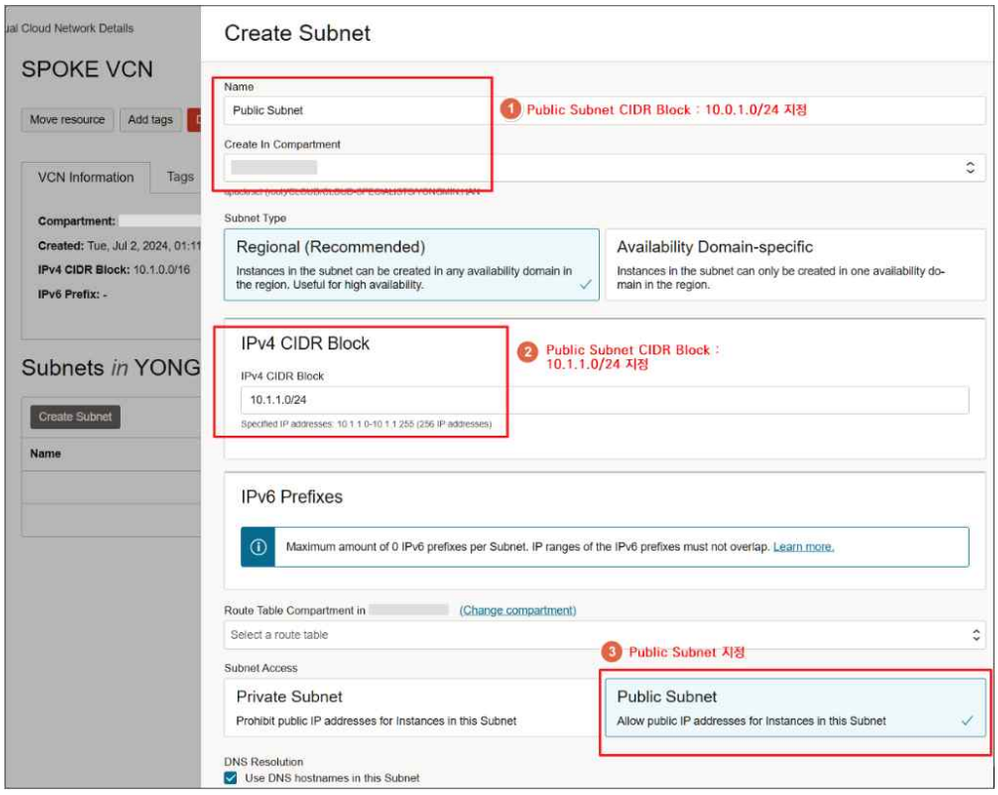
| 그림 2.4.5 | Hub VCN Subnet 생성 화면

- Spoke VCN 생성

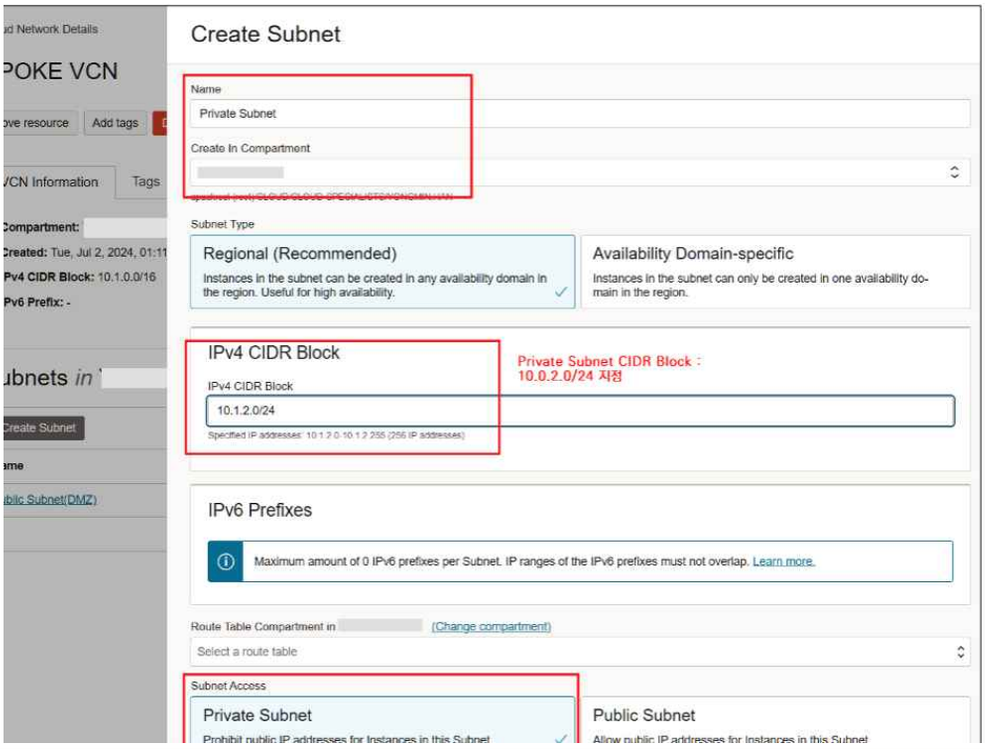


| 그림 2.4.6 | Create VCN

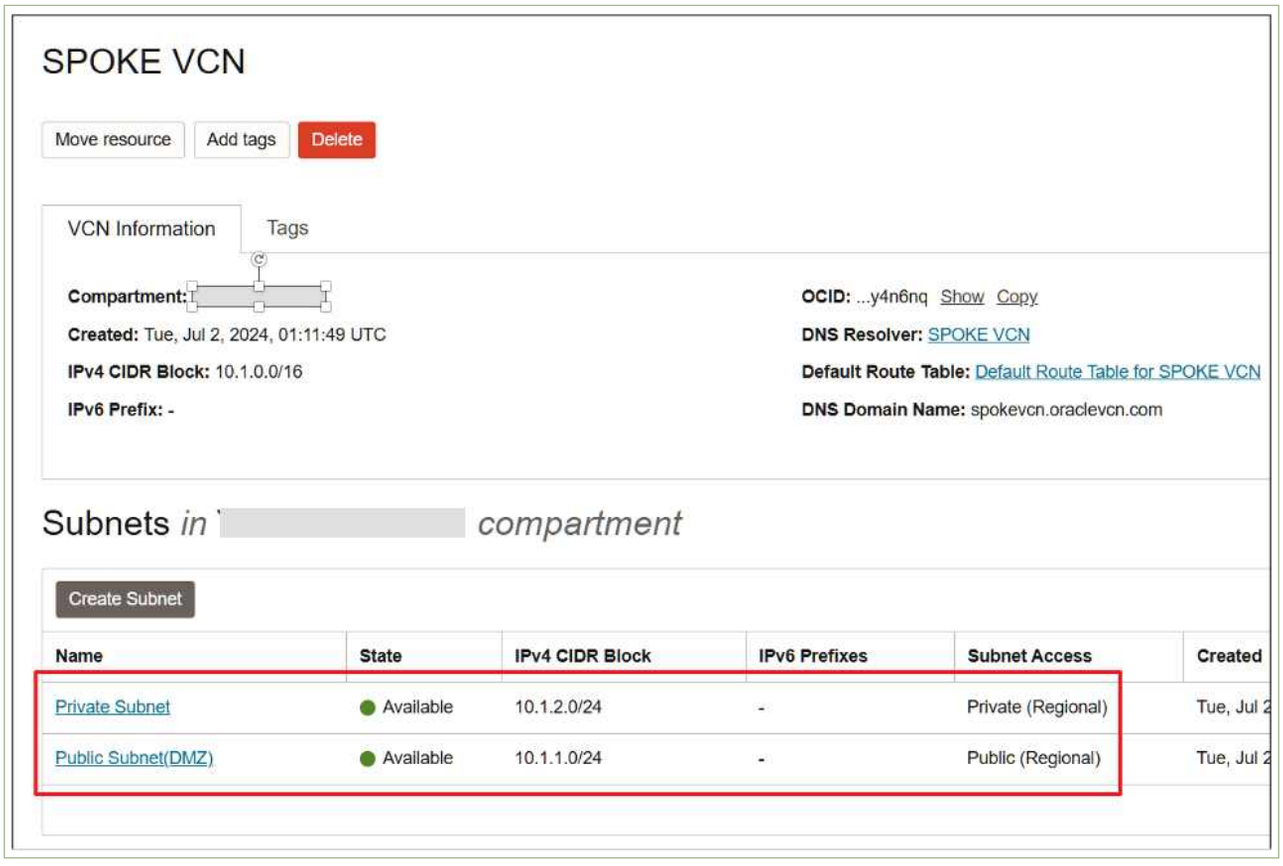
- Spoke VCN Subnet 생성(Public/Private)



| 그림 2.4.7 | Create Subnet(Public)



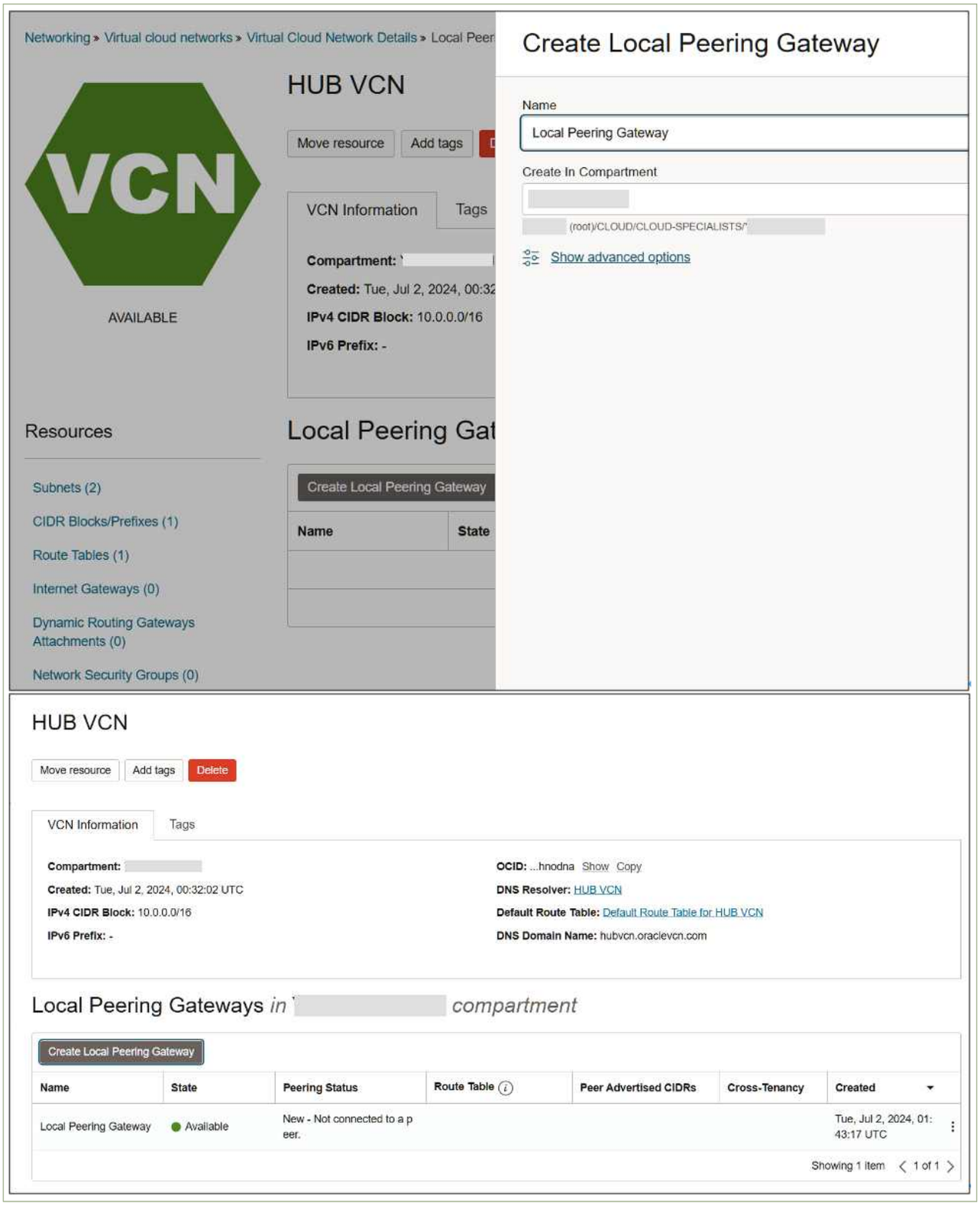
| 그림 2.4.8 | Create Subnet(Private)



| 그림 2.4.9 | Spoke VCN Subnet 생성 화면

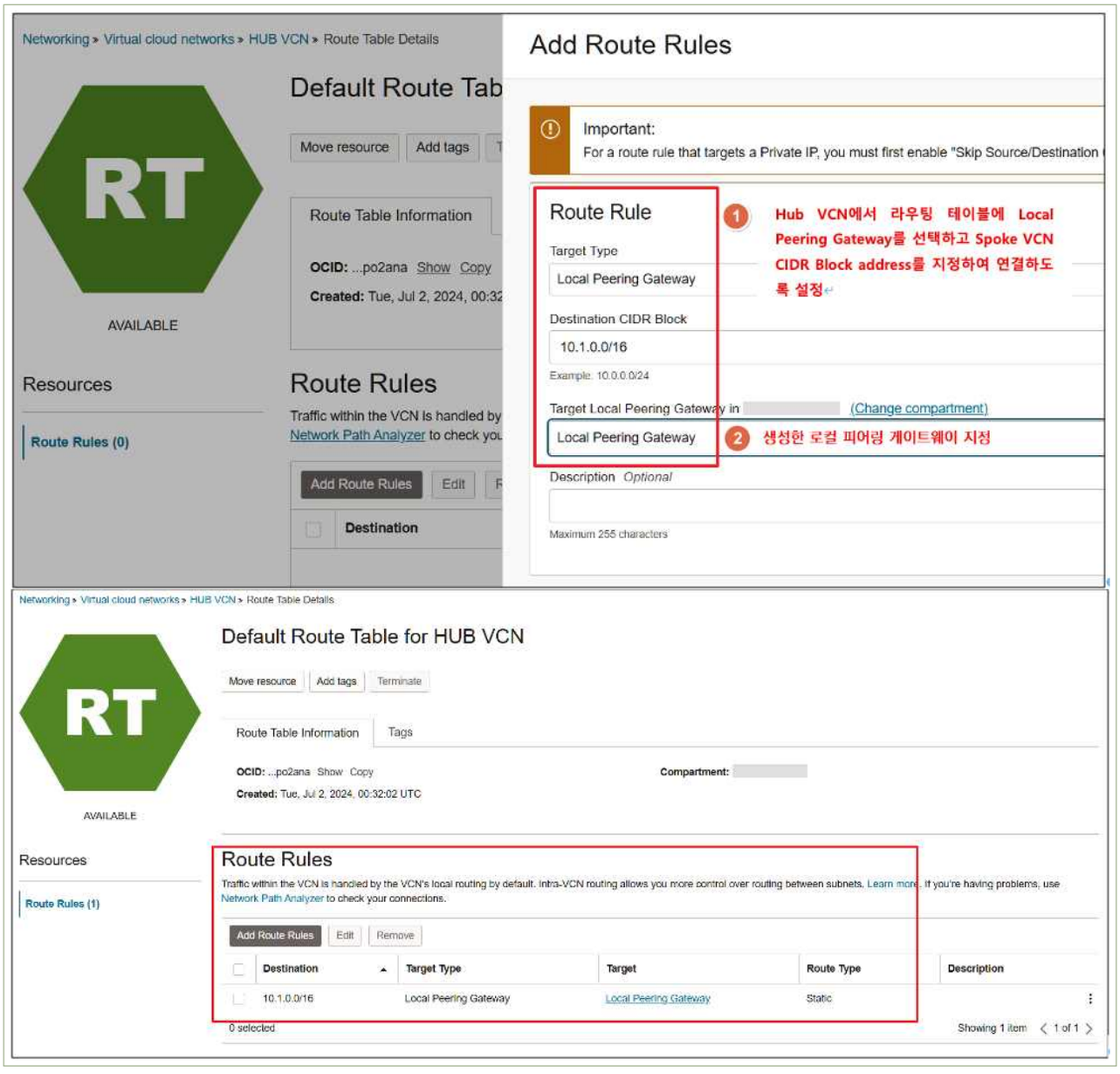
2) 로컬 피어링 게이트웨이(LPG) 및 라우팅 테이블 구성

- 허브(Hub) VCN과 스포크(Spoke) VCN 간에 로컬 피어링 게이트웨이(LPG)를 생성



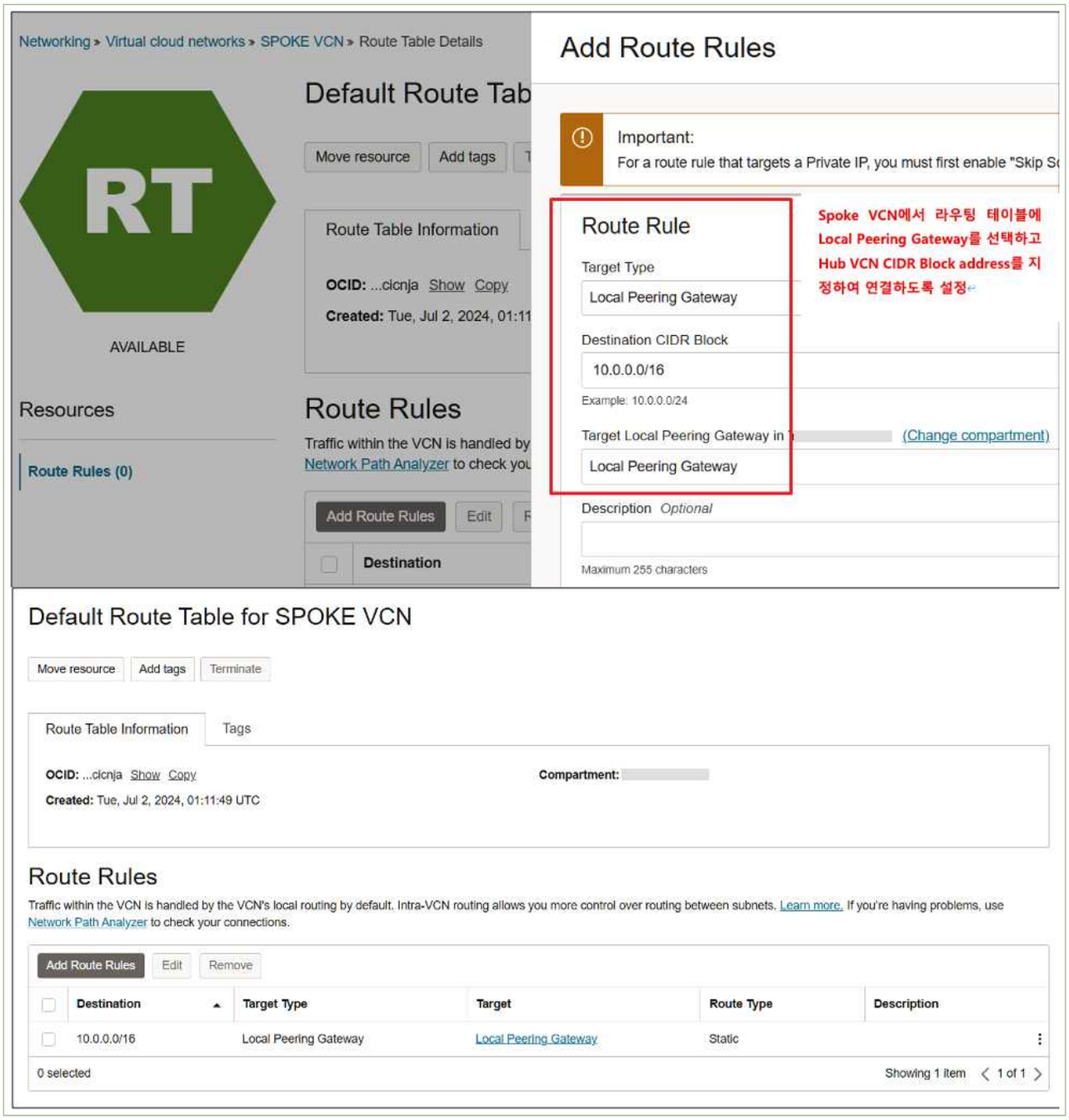
| 그림 2.4.10 | 로컬 피어링 게이트웨이(LPG) 생성

- Hub VCN 라우팅 테이블



| 그림 2.4.11 | 라우팅 설정

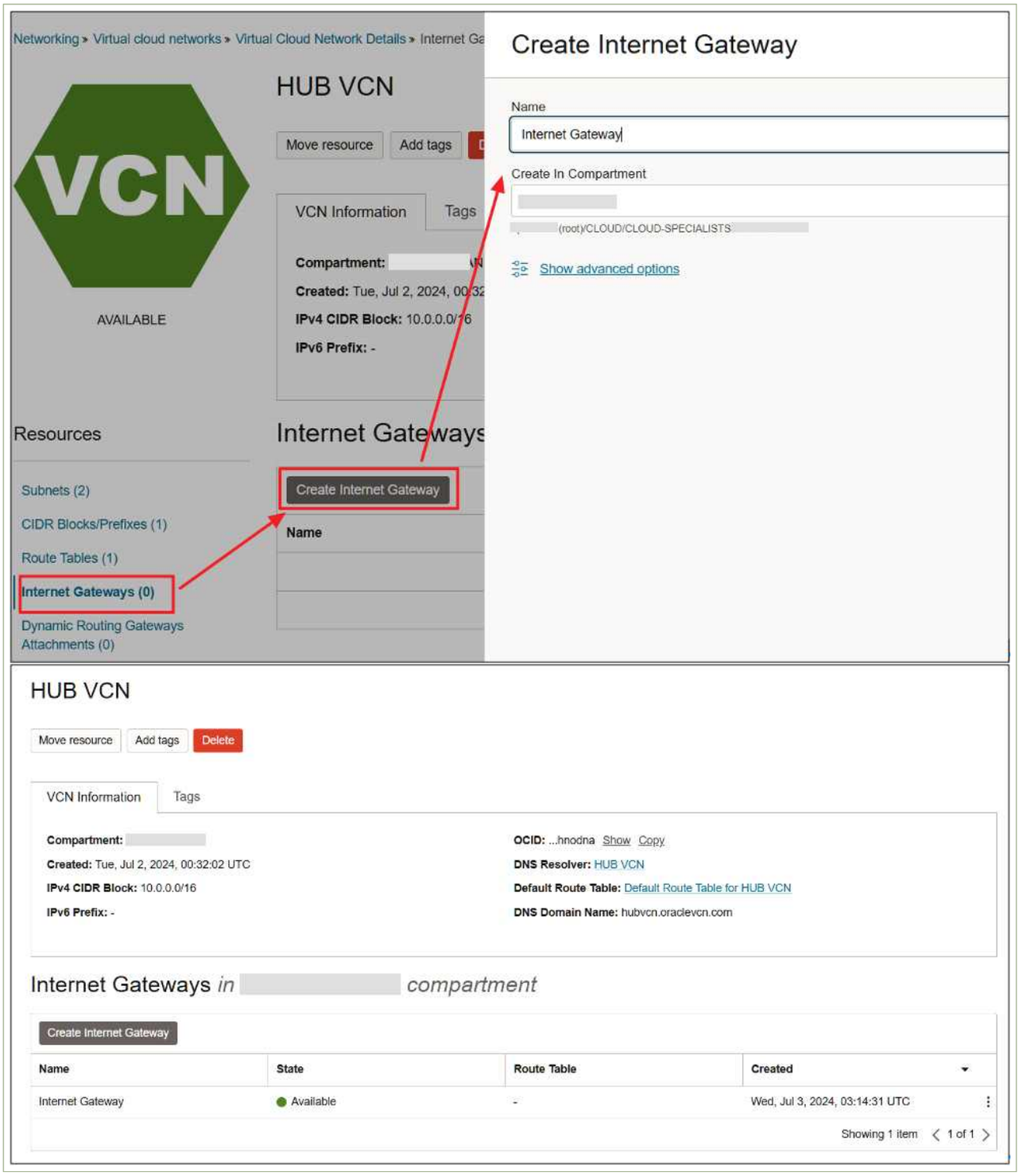
- Spoke VCN 라우팅 테이블



| 그림 2.4.12 | 라우팅 설정

3) 인터넷 게이트웨이(IGW) 설정

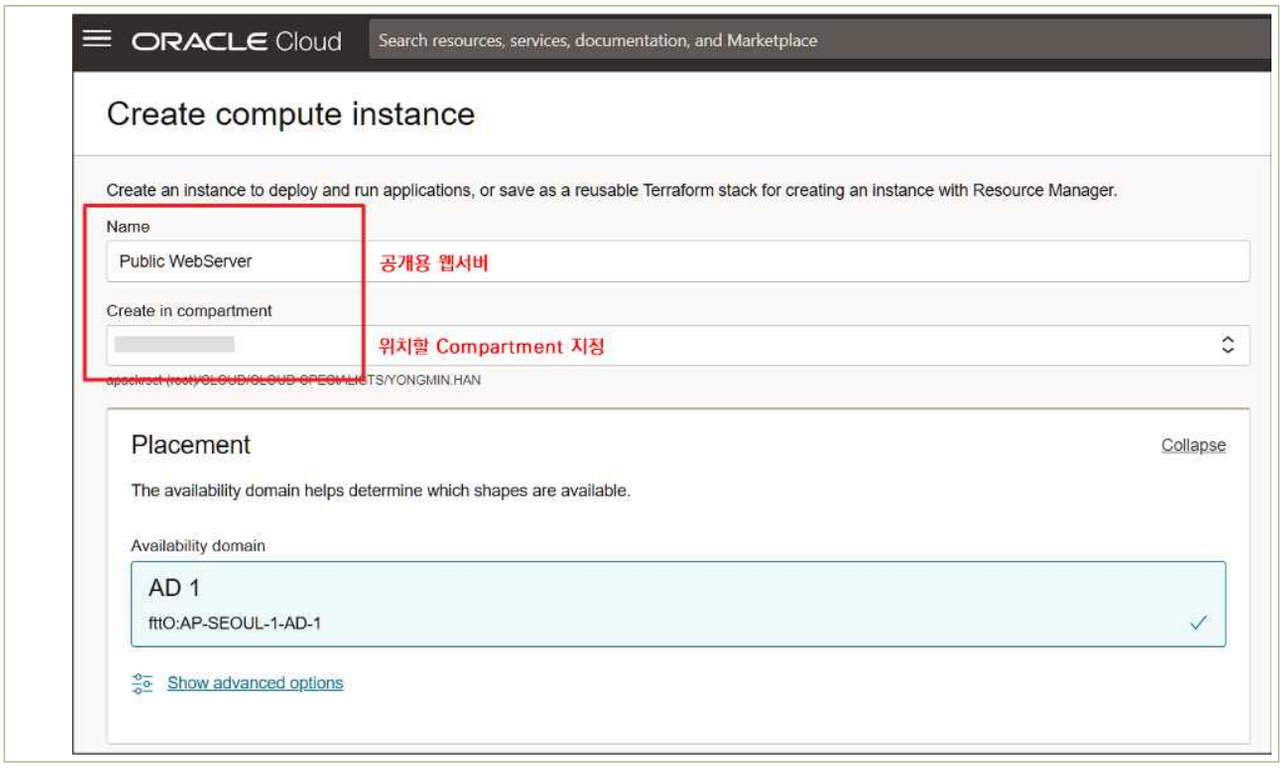
- Hub VCN에 인터넷 게이트웨이(IGW) 생성



| 그림 2.4.13 | 인터넷 게이트웨이(IGW) 설정

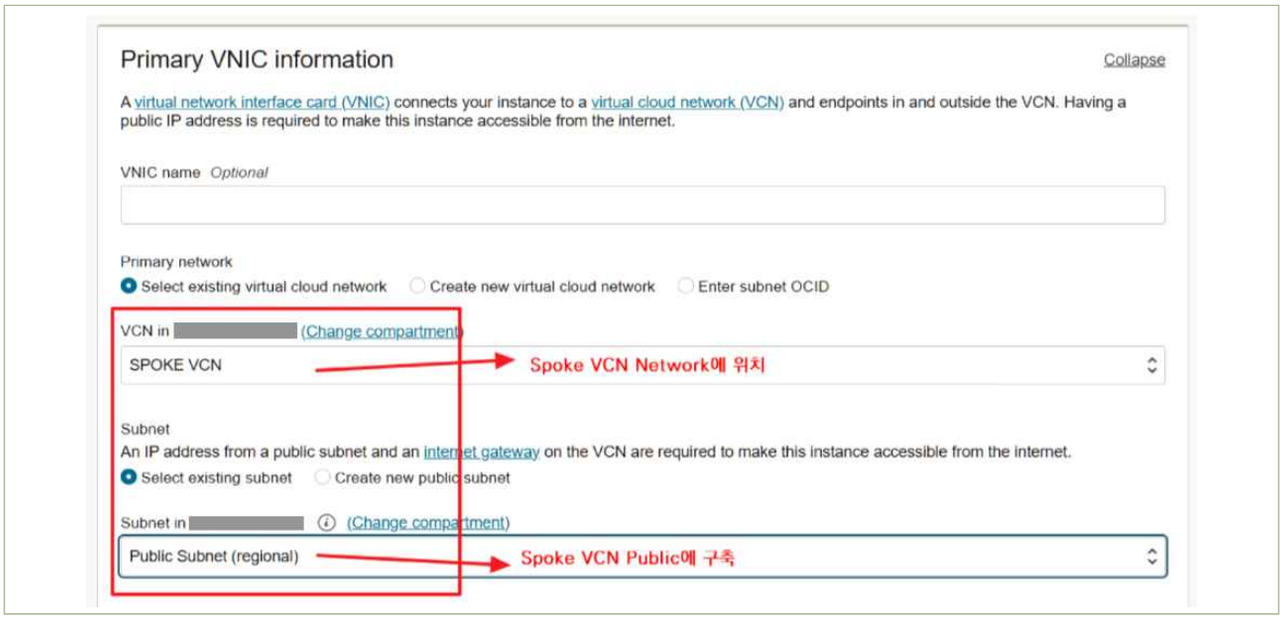
4) 공개용 웹 서버 구축

- Spoke VCN 환경에 공개용 웹 서버를 구성하고, 및 보안 목록(Security List)을 설정

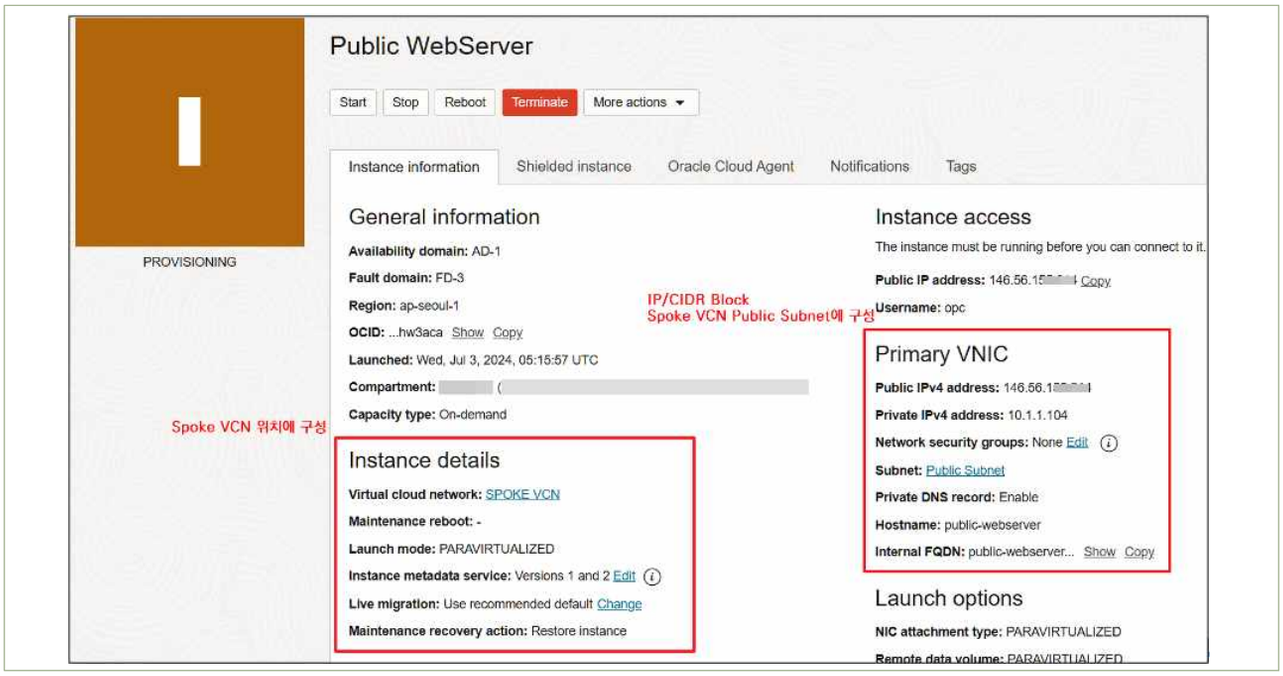


| 그림 2.4.14 | Create computer Instance

- Spoke VCN, Public Subnet에 위치하도록 네트워크 구성 설정

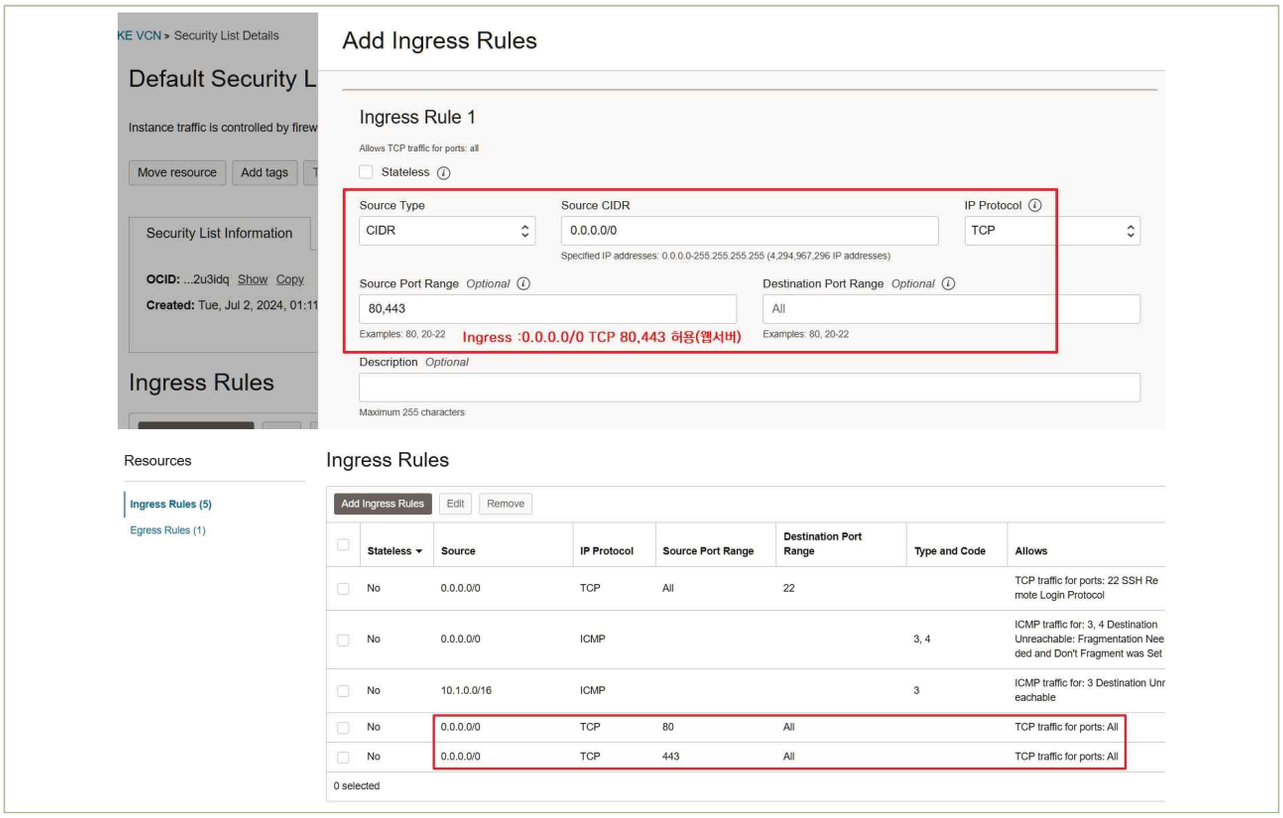


| 그림 2.4.15 | 네트워크 구성



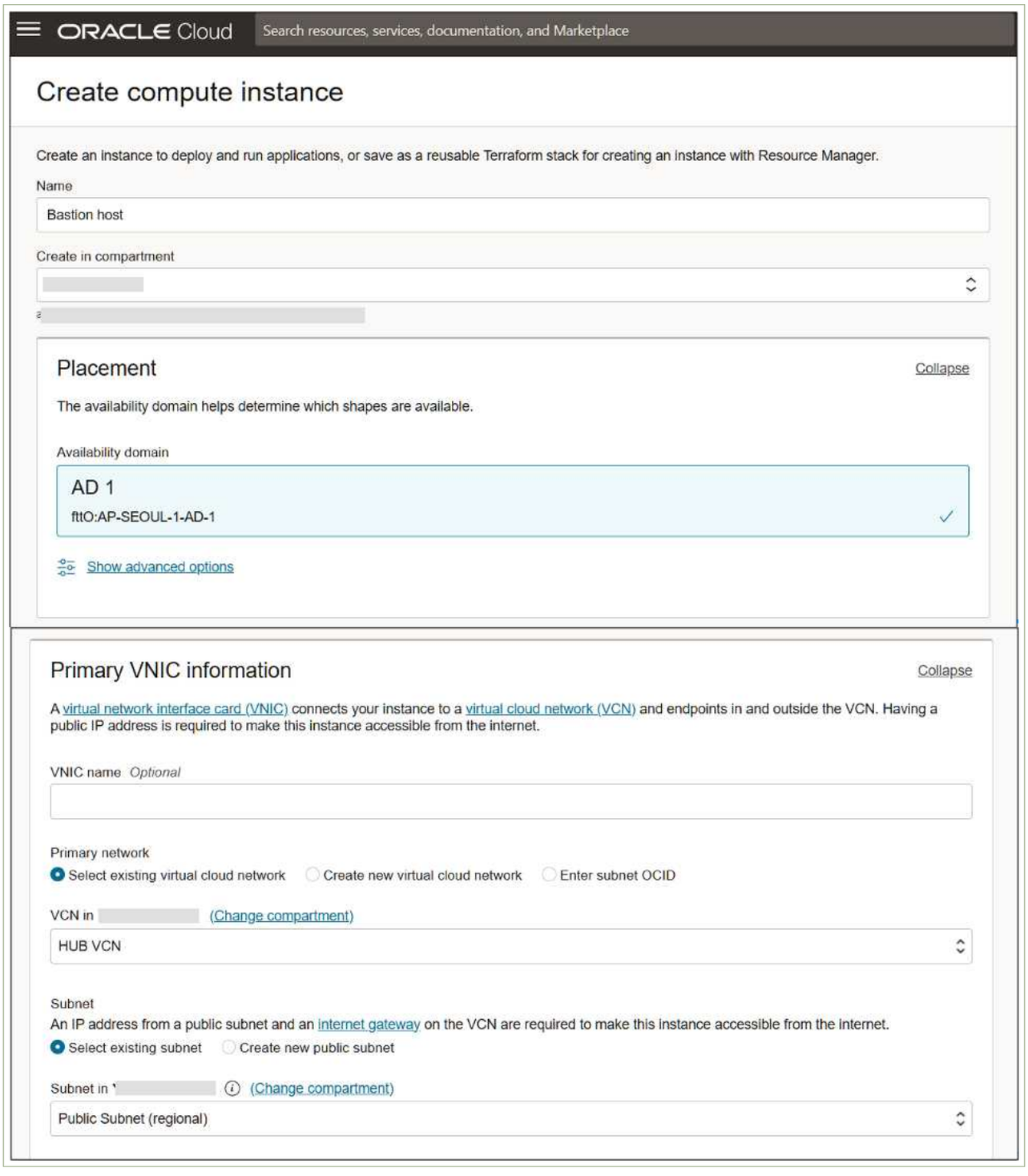
| 그림 2.4.16 | 인스턴스 설정 화면

- 공개용 웹 서버의 TCP 80, 443 포트에 대해, Source IP를 'Any' 대역으로 보안 목록(Security List)을 설정



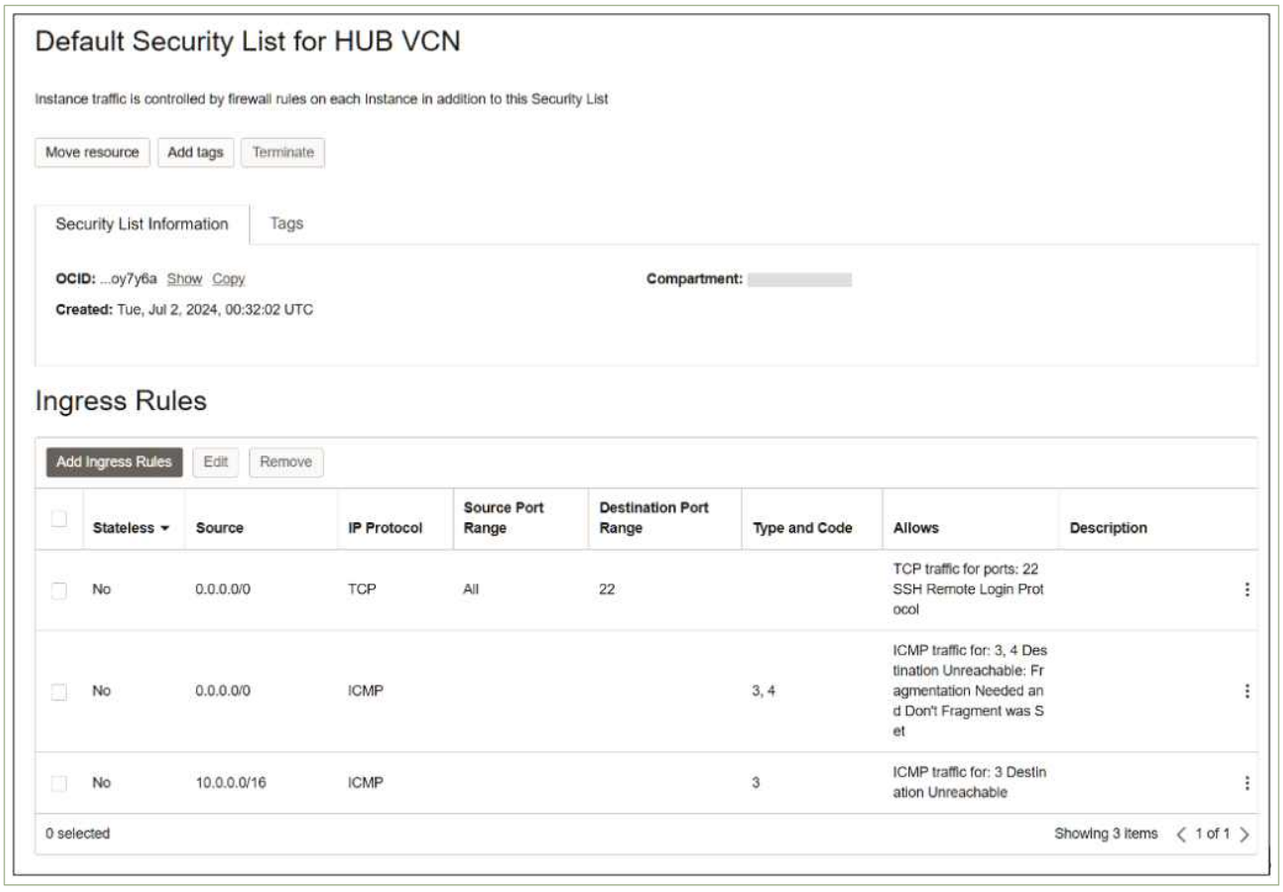
| 그림 2.4.17 | Security List 설정

5) 배스천(Bastion) 호스트를 구성하고 보안 목록(Security List)을 설정



| 그림 2.4.18 | 인스턴스 생성

- 배스천(Bastion) 호스트의 보안 목록(Security List)에 TCP SSH 트래픽을 허용하도록 설정



| 그림 2.4.19 | Security List 설정

4 참고 사항

- [VCN] https://cloud.oracle.com/networking/vcns?region=ap-seoul-1
- [Bastion host] https://cloud.oracle.com/compute/instances?region=ap-seoul-1

1 기준

식별번호	기준	내용
2.5	**네트워크 사설 IP주소 할당 및 관리**	클라우드 환경을 통한 내부망 네트워크 구현 시 사설 IP부여 등으로 보안을 강화하고, 내부IP 유출을 금지하여야 한다.

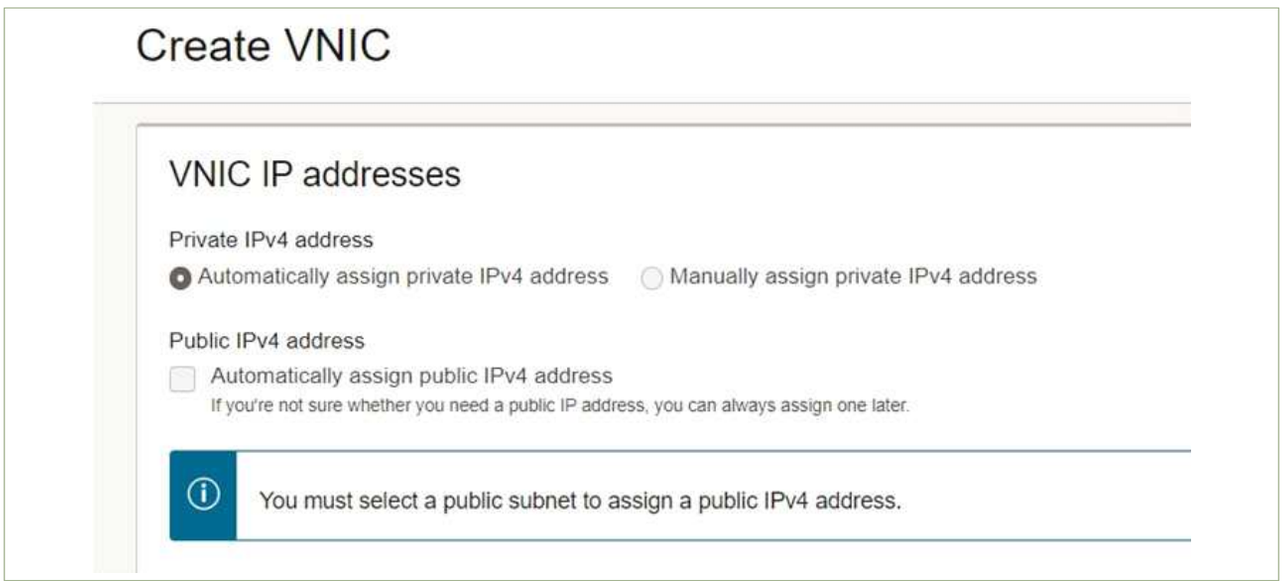
2 설명

- 클라우드 환경 내 내부망 네트워크 구현 시 사설IP를 부여하고 주기적으로 현황을 검토하여야 한다.
  1) 인터넷 게이트웨이, NAT 게이트웨이 등 관련 기능을 통해 사설IP부여 및 IP 관리 수행
  2) 사설 IP 할당 현황에 대한 주기적 검토 수행

3 우수 사례

1) 인터넷 게이트웨이, NAT 게이트웨이 등 관련 기능을 활용하여 사설 IP 부여 및 IP 관리 수행

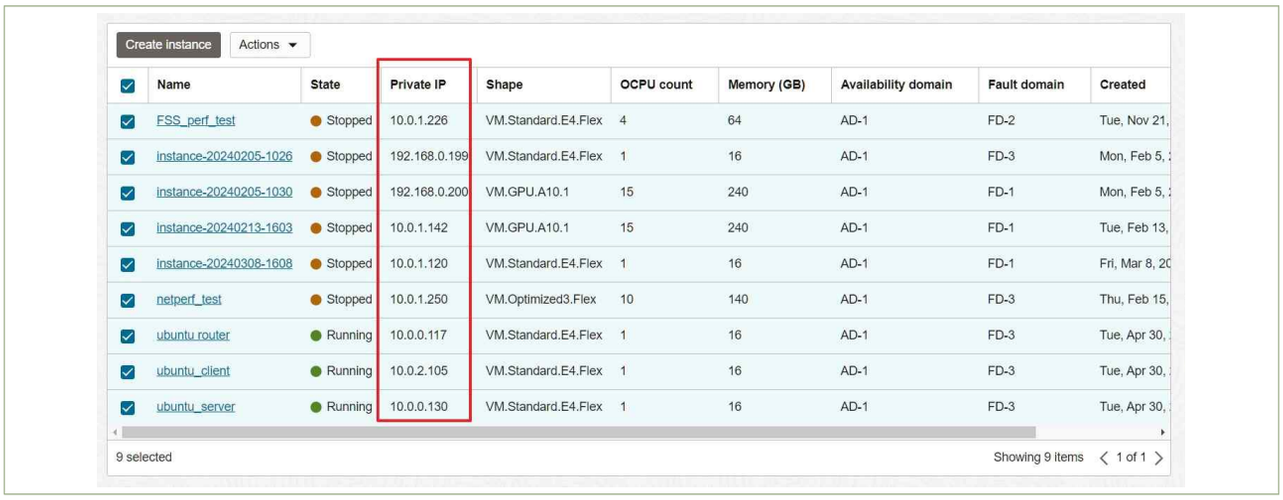
- OCI의 프라이빗 서브넷(Private Subnet)에 인스턴스를 생성하면 공인 IP(Public IP)를 할당할 수 없도록 설계되어 있음



| 그림 2.5.1 | VNIC 생성

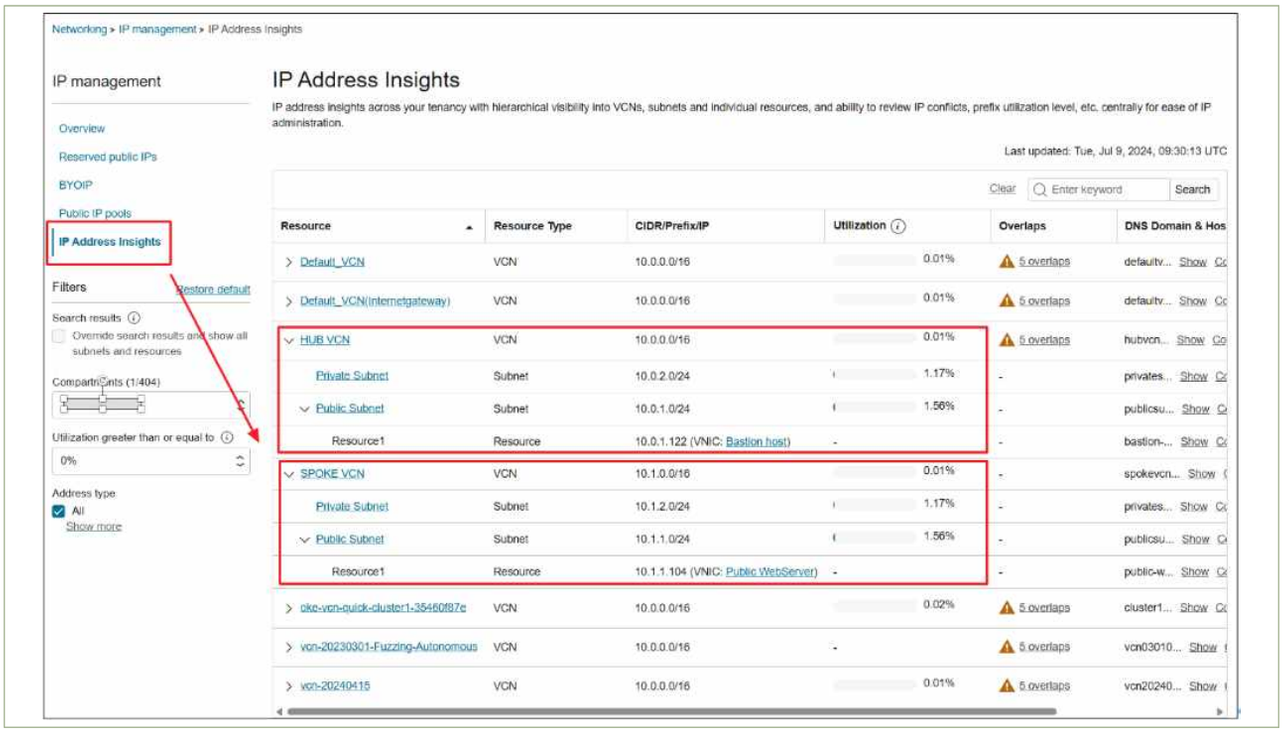
2) 사설 IP 할당 현황에 대한 주기적 검토 수행

- (가상 자원 관리시스템) '홈' → 'Networking' → 'Virtual Cloud Networks' → 'VCN선택' → 'Virtual cloud network details' → 'CIDR Blocks/Prefixes'
  - CIDR Blocks/Prefixes에서 Private IP Address Rage를 지정 및 확인 가능
  - Compute → Instances에서 선택한 컴파트먼트(Compartment)의 전체 목록에서 Private IP 현황을 확인
  - Actions(Table settings) 메뉴에서 정렬 및 항목을 추가/삭제하도록 지원



| 그림 2.5.2 | Private IP 현황

- (OCI 콘솔) '홈' → 'Networking' → 'IP management' → 'IP Address Insights'에서 VCN 내에 할당된 네트워크 서브넷과 리소스를 테이블 형태로 확인할 수 있음



| 그림 2.5.3 | IP Address Insights

4 참고 사항

- [VCN] https://cloud.oracle.com/networking/vcns?region=ap-seoul-1
- 관리하고자 하는 VCN 선택 → Virtual Cloud Network details → CIDR Blocks/Prefixes

1 기준

식별번호	기준	내용
2.6	**네트워크(방화벽 등) 정책 주기적 검토**	클라우드 서비스를 통해 구현한 네트워크 정책에 대해 주기적 검토를 수행하여야 한다.

2 설명

- 클라우드 네트워크 관련 서비스 정책에 대한 적정성 여부를 주기적으로 검토하여야 한다.
  1) 방화벽 정책에 관한 주기적 검토 수행
  2) ACL 정책에 관한 주기적 검토 수행
  3) 보안그룹에 관한 주기적 검토 수행

3 우수 사례

- '2. 네트워크 관리' 분야의 내용을 참고하여 내부에서 방화벽, ACL, 보안 그룹 등에 대해 검토

4 참고 사항

- N/A

3. 계정 및 권한 관리

3.1. 클라우드 계정 권한 관리
3.2. 이용자별 인증 수단 부여
3.3. 인사변경 사항 발생 시 계정 관리
3.4. 클라우드 가상자원 관리 시스템 관리자 권한 추가 인증 적용
3.5. 클라우드 OCI 콘솔 로그인 규칙 수립
3.6. 계정 비밀번호 규칙 수립
3.7. 공개용 웹 서버 접근 계정 제한

3 계정 및 권한 관리

1 기준

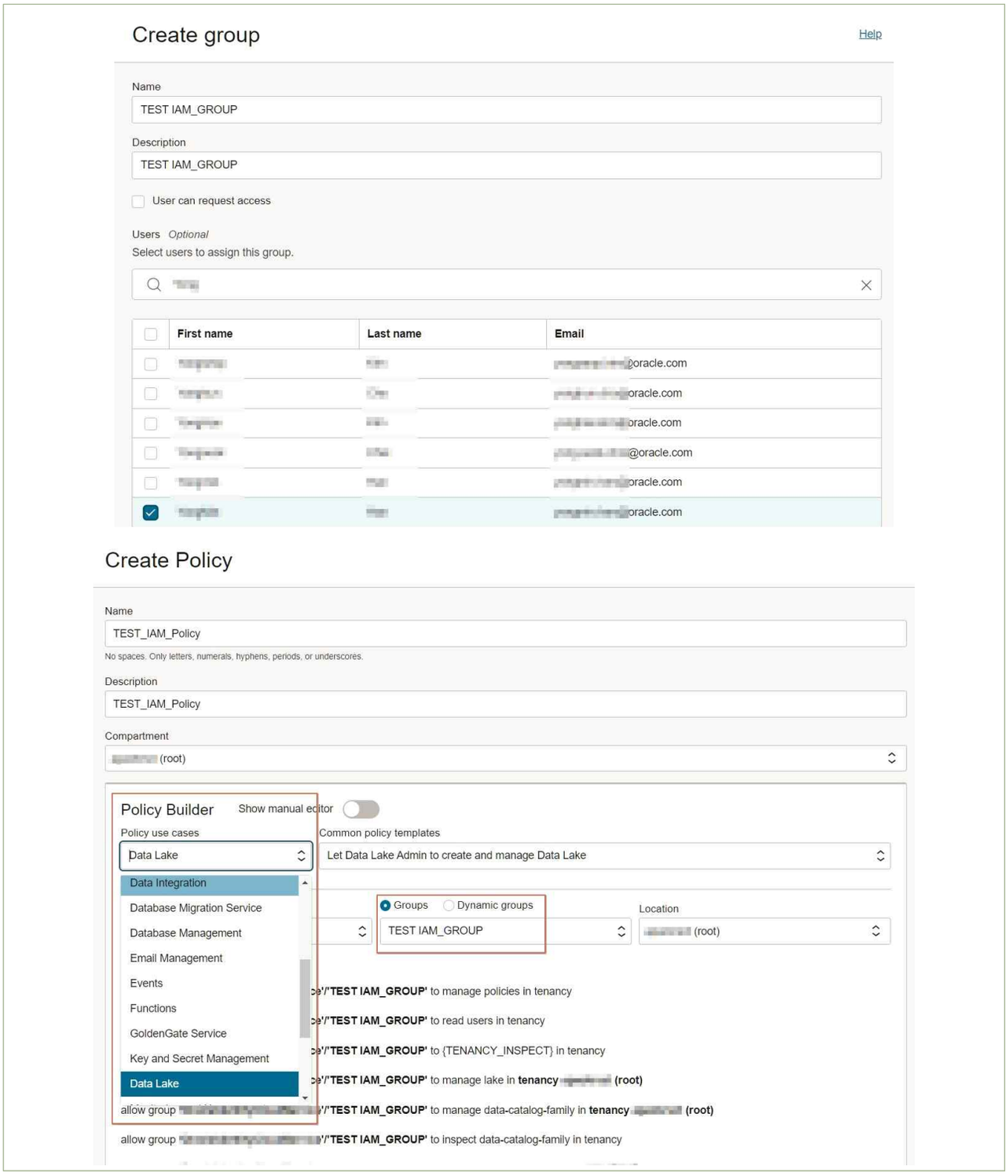
식별번호	기준	내용
3.1	**클라우드 계정 권한 관리**	클라우드 서비스 이용 시 업무 및 권한에 따라 계정을 관리하여야 한다.

2 설명

- 클라우드를 이용하는 임직원의 업무 및 권한에 따라 계정을 관리하여야 한다.
  1) 자격 증명 등의 기능을 이용하여 계정 권한 관리
  2) 사전에 정의된 행위만이 가능하도록 역할을 생성
- 콘솔 최상위 관리자(ex. 최초 가입계정 등)은 서비스 운영에 활용하지 않아야 한다.
  1) 부득이 일부 서비스에 대해 관리자 권한이 필요한 경우, 신규로 계정을 생성하여 필요한 권한을 부여한 후 활용
  2) 예외적으로 반드시 최초 콘솔 가입계정을 이용하여야 하는 특정 서비스의 경우에는 MFA 등 추가 인증 방식을 구현하고 접속 IP를 제한하는 등 강화된 보안환경 구성

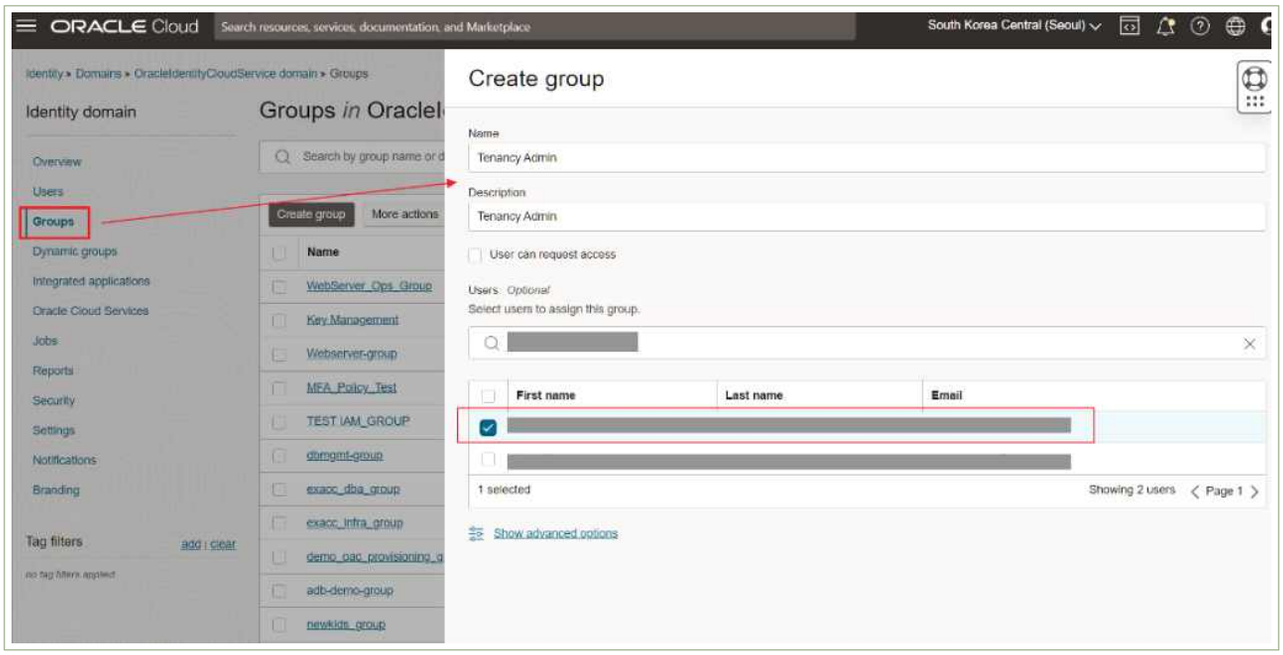
3 우수 사례

- (OCI 콘솔) ‘홈’ → ‘Identity & Security’ → ‘Identity’ → ‘Domain’ → ‘도메인 선택’ → ‘Users’ → ‘Create Group’에서 이용자의 역할별(Dev, Ops, Sec 등) 그룹을 생성하고, 각 그룹에 역할과 권한을 부여 가능



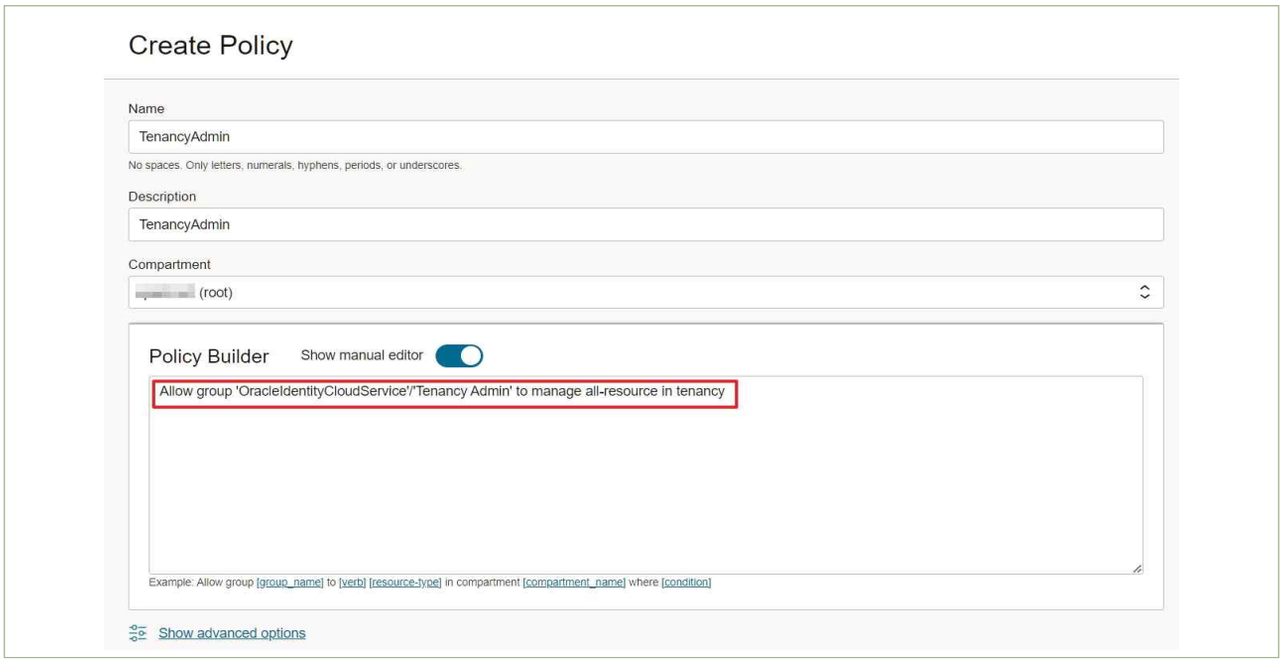
| 그림 3.1.1 | 자격 증명에서 역할 지정 및 권한 관리

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Groups'에서 최상위 관리자를 별도 그룹으로 지정하고, 해당 그룹이 서비스 운영에서 제외되도록 설정
  - 최상위 관리자 그룹을 생성하고, 최상위 관리자를 해당 그룹에 할당



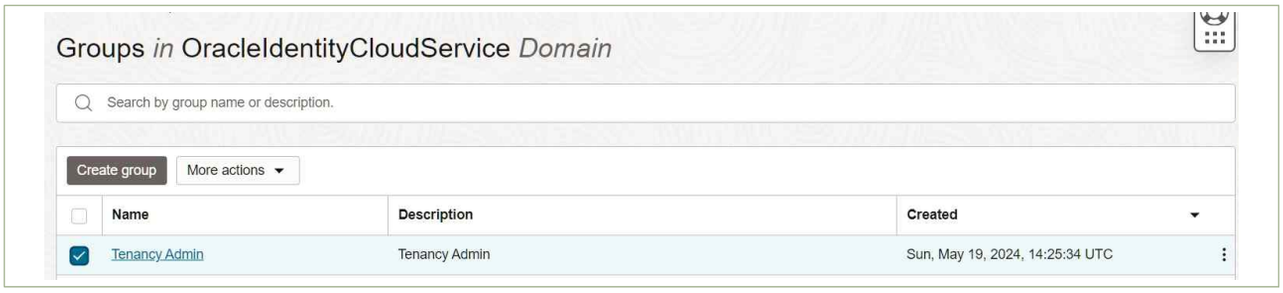
| 그림 3.1.2 | Create Group

- 태넌시 관리자(Tenancy Admin) 그룹에 모든 권한 부여
- [정책 예시] 'Allow group 〈그룹 이름〉 to manage all-resources in tenancy'



| 그림 3.1.2 | 정책 생성(Create Policy)

- 최상위 관리자는 클라우드 서비스 운영에 직접 관여하지 않도록 별도로 관리



| 그림 3.1.3 | 그룹(Group) 생성 화면

4 참고 사항

- https://cloud.oracle.com/identity/domains/overview?region=ap-seoul-1

1 기준

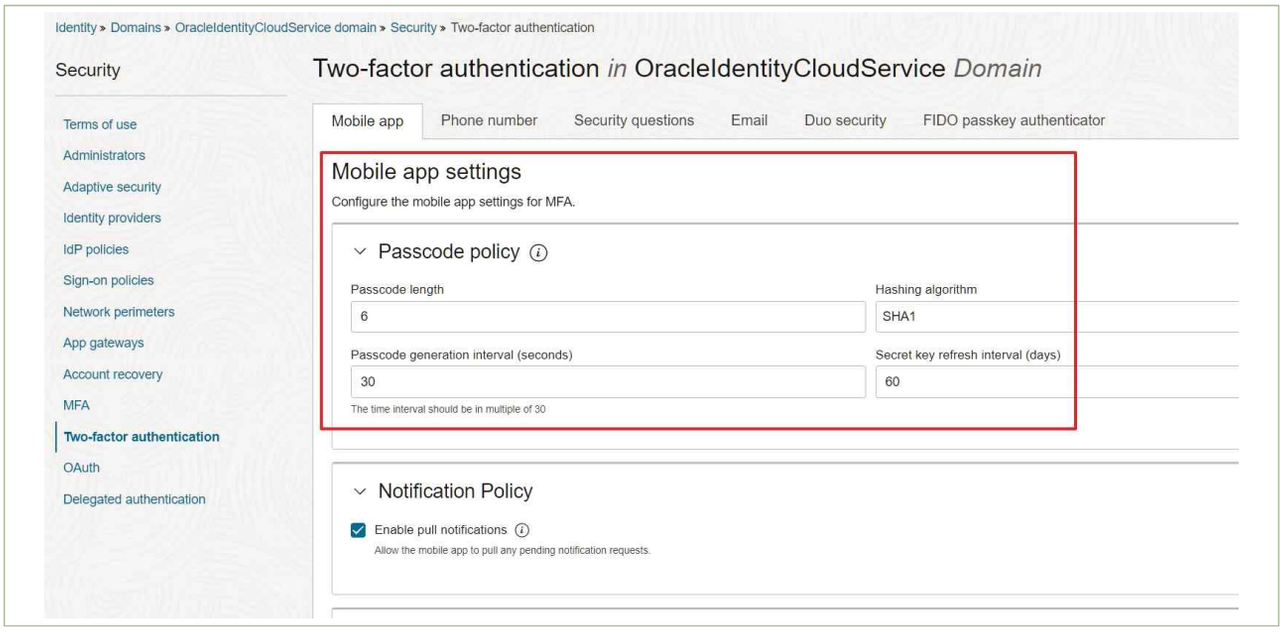
식별번호	기준	내용
3.2	**이용자별 인증 수단 부여**	클라우드 서비스를 이용하는 임직원(이용자)별 인증 수단을 할당하여야 한다.

2 설명

- 클라우드 서비스를 이용하는 임직원(이용자)별 인증 수단을 부여하여야 하며, 필요 시 추가인증을 적용할 수 있어야 한다. (외부직원 포함)
  1) IAM(Identity and Access Management) 기능 등을 이용하여 이용자별 인증수단 적용
  2) 업무 중요도에 따른 MFA 추가 인증(OTP, 바이오 인증 등) 고려

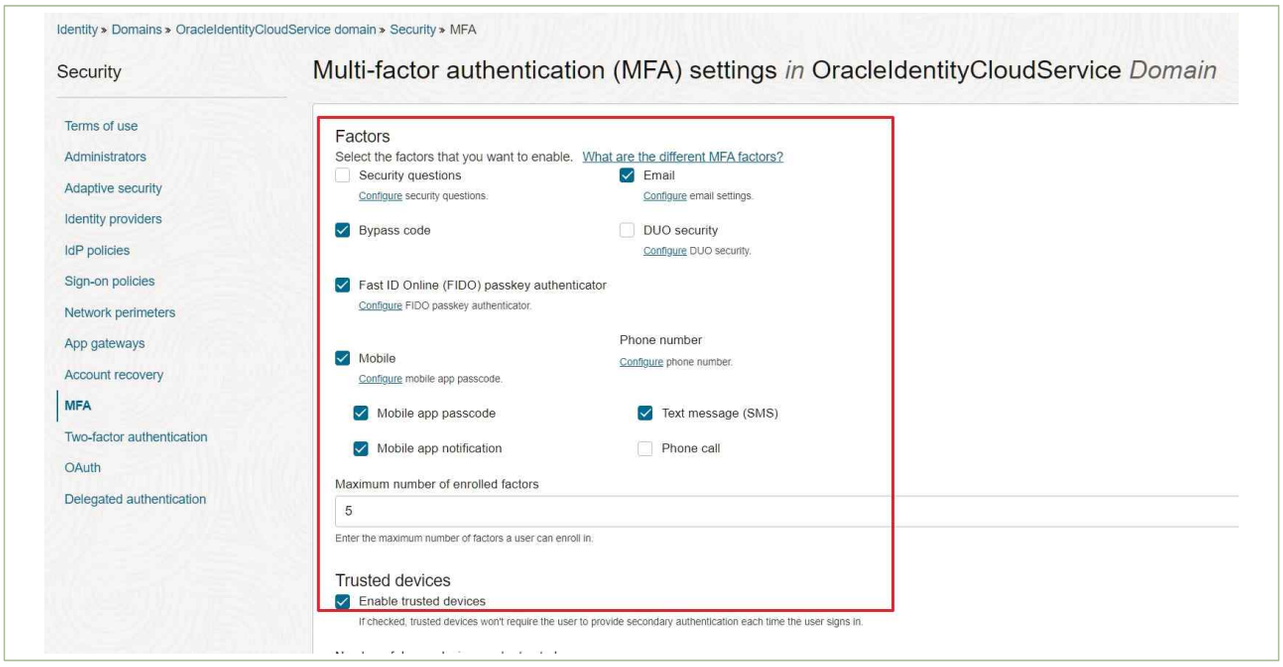
3 우수 사례

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Security' → 'Two-factor authentication'에서 인증수단(Mobile-app, Phone, Email 등) 정책 부여 가능



| 그림 3.2.1 | 도메인 이용자별 인증 수단 부여

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Security' → 'MFA'에서 다중 인증(MFA) 설정이 가능



| 그림 3.2.2 | 다중 인증(MFA) 설정

4 참고 사항

- https://cloud.oracle.com/identity/domains/overview?region=ap-seoul-1

1 기준

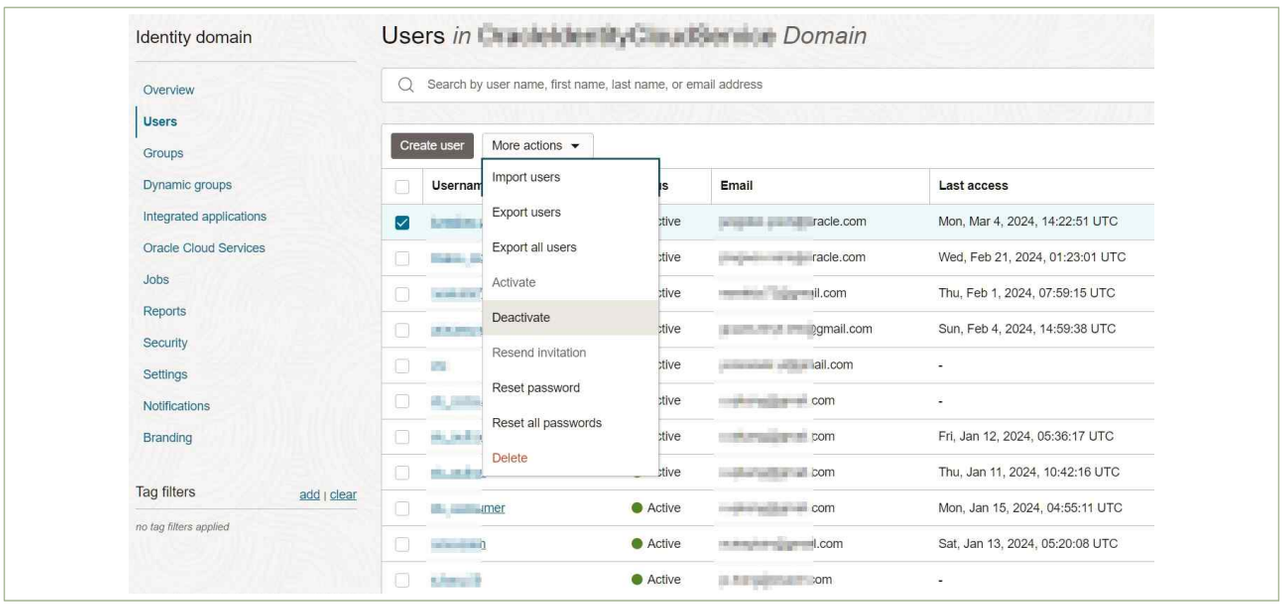
식별번호	기준	내용
3.3	**인사변경 사항 발생 시 계정 관리**	이용자의 인사변경(휴직, 전출, 퇴직 등) 발생 시 지체 없이 이용자 계정 삭제, 중지 등의 조치를 수행하여야 한다.

2 설명

- 클라우드를 이용하는 임직원의 인사변경 사항 발생 시 지체없이 이용자 계정 삭제, 중지 등의 조치를 수행하여야 한다.
  1) 인사변경이 발생한 이용자의 계정 삭제 또는 중지
  2) 인사변경이 발생한 이용자가 공용 계정 이용 시 계정 비밀번호 변경 등

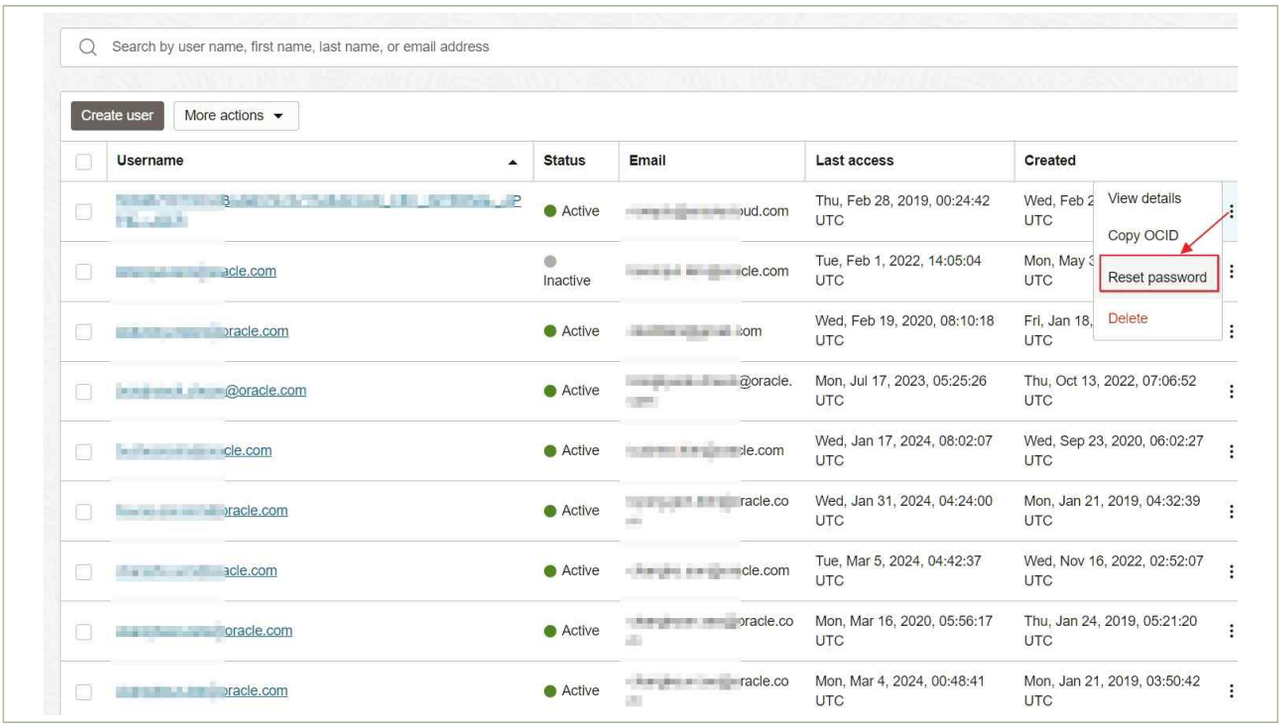
3 우수 사례

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Users' → 'User list' → '계정 선택' → 'More actions' → 'Delete or Deactivate'에서 인사변경이 발생한 이용자의 계정을 삭제하거나 비활성화(Deactivate)할 수 있음



| 그림 3.3.1 | 이용자 계정 상태 변경

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Users' → 'User list' → '계정 오른쪽 옵션 버튼 클릭' → 'Reset password'



| 그림 3.3.2 | 공용 계정 비밀번호 변경

- API(CLI)에서 '--user-id [text]' 매개변수를 이용해 사용자 계정 생성, 삭제 등 계정 상태를 변경할 수 있음

```
예) oci iam user delete [OPTIONS]
# oci iam user delete --user-id $user_id
```

| 그림 3.3.3 | 이용자 계정 상태 변경

- https://docs.oracle.com/en-us/iaas/tools/oci-cli/3.37.11/oci_cli_docs/cmdref/iam.html
  https://docs.oracle.com/en-us/iaas/tools/oci-cli/3.37.11/oci_cli_docs/cmdref/iam/user/delete.html

4 참고 사항

- https://cloud.oracle.com/identity/domains/overview?region=ap-seoul-1

1 기준

식별번호	기준	내용
3.4	**클라우드 가상자원 관리시스템 관리자 권한 추가인증 적용**	클라우드 서비스 관리자 권한으로 로그인 시 추가인증 수단을 적용하여야 한다.

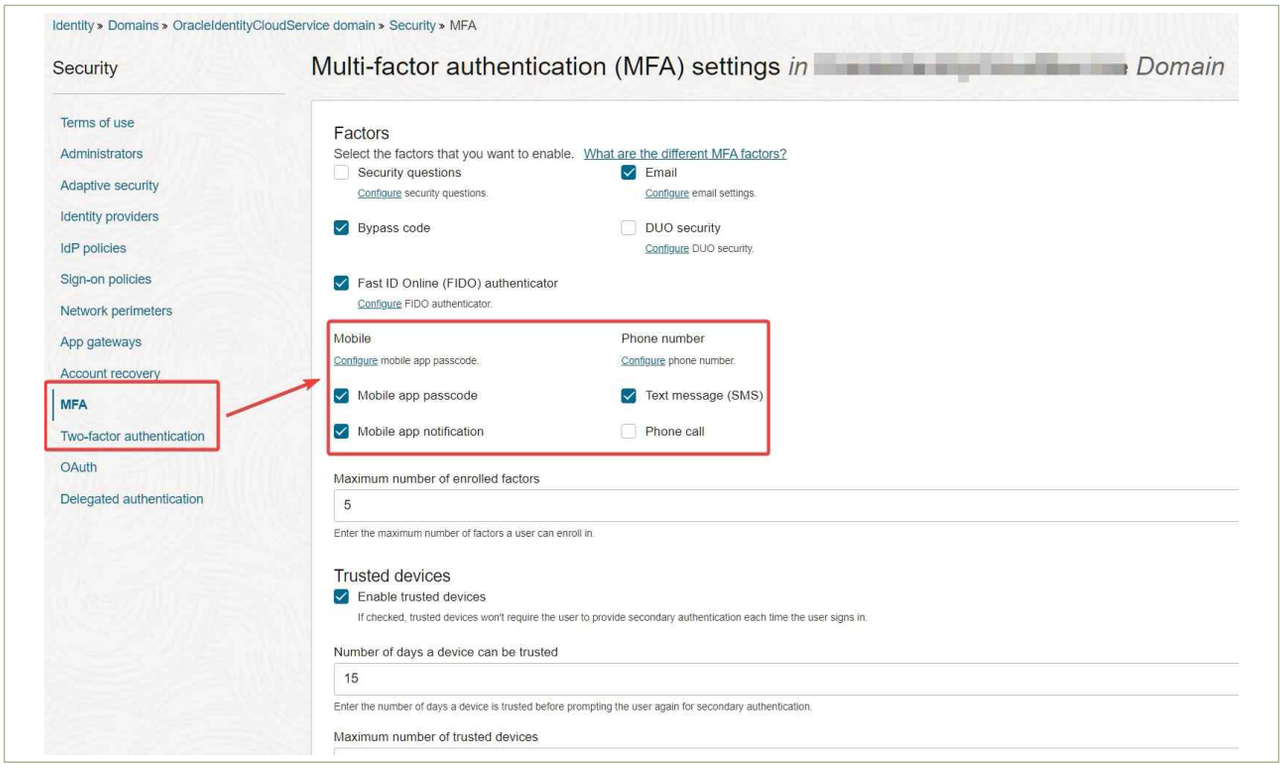
2 설명

- 이용자는 패스워드 무작위 대입 공격 등에 대응하기 위해 가상자원 관리시스템 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.
  1) 이메일 인증
  2) SMS 인증
  3) 별도 인증도구(OTP, 바이오 인증 등) 활용 등

3 우수 사례

1) (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Security' → 'MFA'에서 Mobile, Phone(SMS), Email 등 Multi-factor 인증 등 추가 보안 요소 등록

- 1단계 : 아이덴티티 도메인(ID)에서 MFA를 활성화



| 그림 3.4.1 | MFA Settings 화면

1. Mobile (Oracle Mobile Authentication) 인증

(1) OMA 모바일 앱 다운로드 :

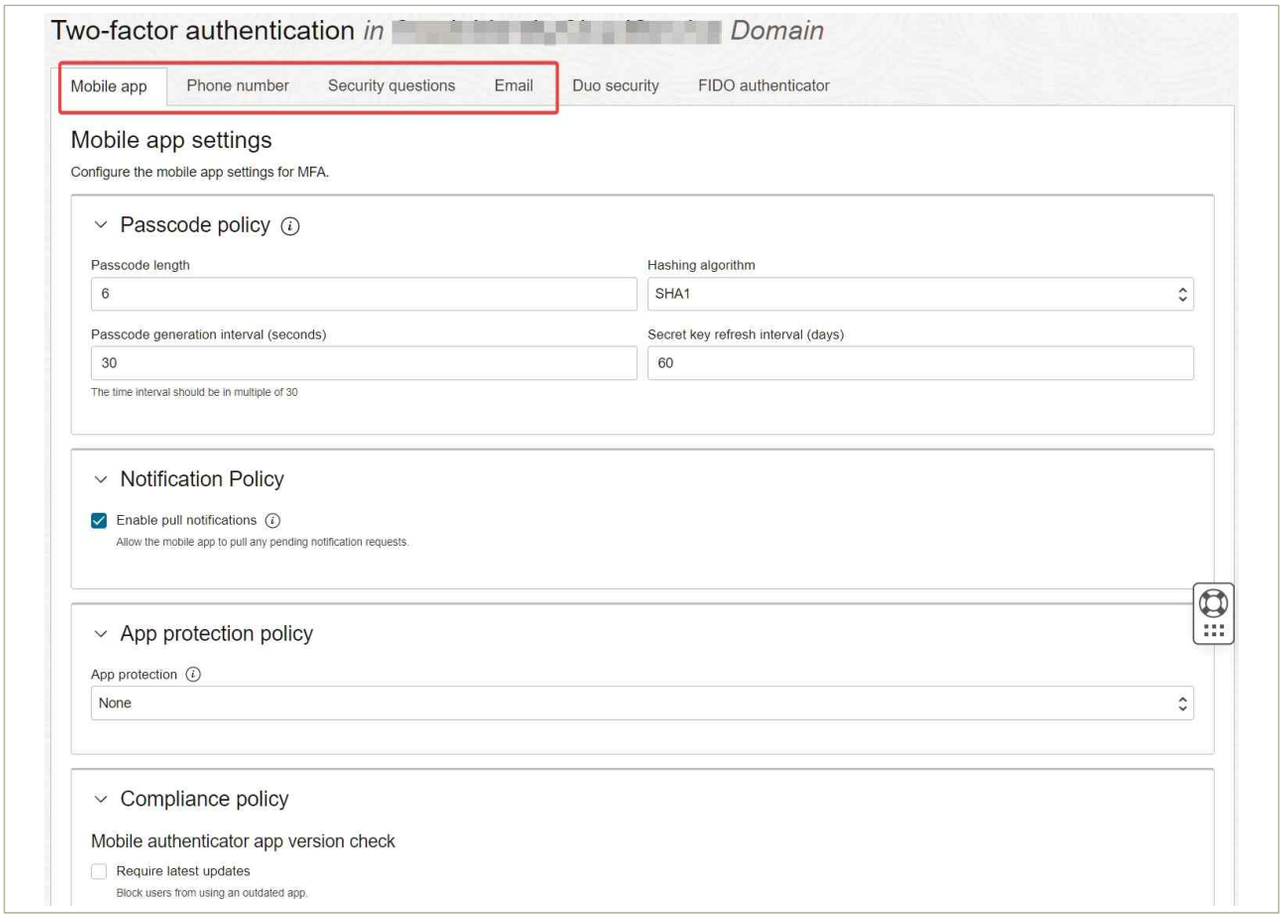
- 2단계 인증(2FA) 등록 절차 외에 OMA 앱을 모바일 기기에 다운로드하는 절차
- https://docs.oracle.com/en-us/iaas/Content/Identity/mobileauthapp/download-mobile-authenticator-app.htm#download-mobile-authenticator-app

(2) 신규 및 기존 모바일 기기 재등록 :

- Mobile app notification : 2단계 인증 요청 시 모바일 기기의 알림에서 인증 버튼을 클릭하여 인증
- Mobile app passcode : 모바일 기기에서 OTP 인증 코드를 확인한 후, 인증 화면에 OTP 코드를 입력하여 인증
- https://docs.oracle.com/en-us/iaas/Content/Identity/mobileauthapp/registering_mobile_devices_with_oma.htm#registering_mobile_devices_with_oma

(3) OMA 관리자 앱 관리

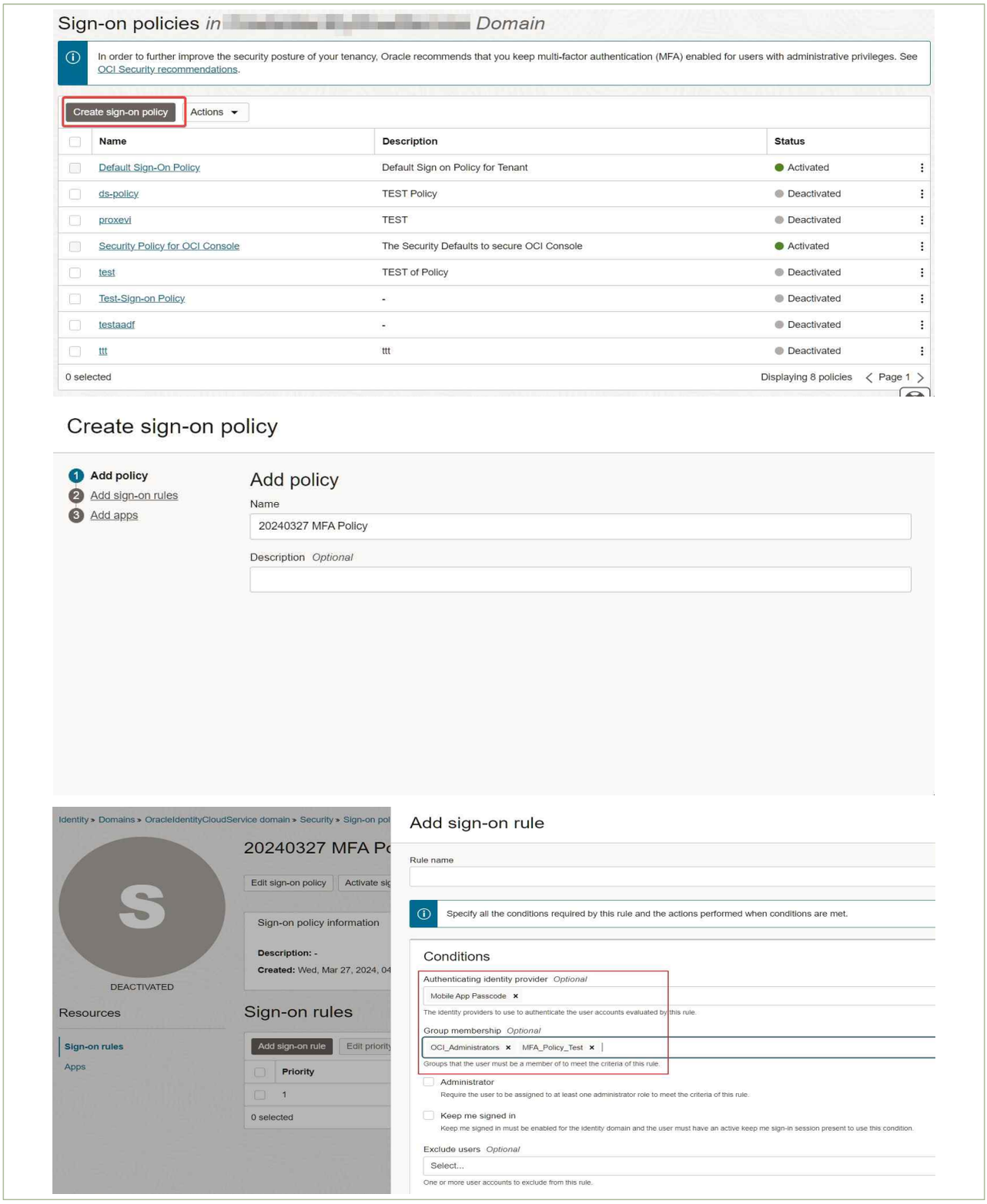
- OMA 앱을 사용하면 계정 보기, PIN 관리, 알림 관리와 같은 기능을 쉽게 맞춤 설정할 수 있음
- https://docs.oracle.com/en-us/iaas/Content/Identity/mobileauthapp/manage-oracle-mobile-authenticator-app.htm#manage-oracle-mobile-authenticator-app



| 그림 3.4.2 | Two-factor authentication 설정 화면

2) (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인선택' → 'Security' → 'Sign-on policies' → 'Create Sign-on policy'

- 2단계 : 새 로그인 정책(Sign-on policy) 만들기



| 그림 3.4.3 | Sign-on Policy 생성

- Authentication identity provider → Mobile app passcode 등 지정
- Group membership : 기존에 생성된 그룹(Group)을 지정

4 참고 사항

- https://cloud.oracle.com/identity/domains/overview?region=ap-seoul-1
- https://docs.oracle.com/en-us/iaas/Content/Security/Reference/iam_security_topic-iam_mfa_with_identity_domains.htm#iam_security_topic-iam_mfa_with_identity_domains

1 기준

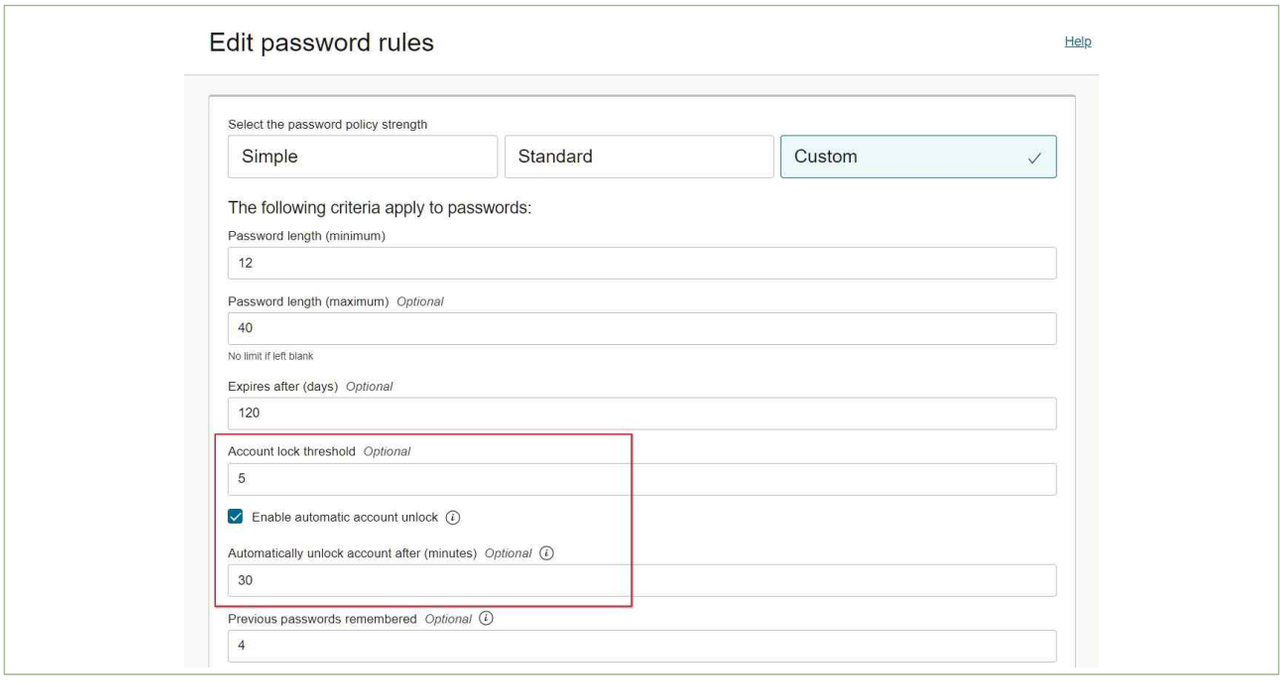
식별번호	기준	내용
3.5	**클라우드 가상자원 관리시스템 로그인 규칙 수립**	이용자 가상자원 관리시스템 접근 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.

2 설명

- 이용자는 패스워드 무작위 대입 공격 등에 대응하기 위해 가상자원 관리시스템 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.
  1) 로그인 오류에 따른 보안통제 방안 수립 등

3 우수 사례

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Setting' → 'Password policy' → '생성한 패스워드 정책' → 'Edit password rules'에서 안전한 로그인 규칙 수립 가능



| 그림 3.5.1 | 무차별 공격에 대응하는 계정 잠금 설정

4 참고 사항

- https://cloud.oracle.com/identity/domains/overview?region=ap-seoul-1

1 기준

식별번호	기준	내용
3.6	**계정 비밀번호 규칙 수립**	클라우드 가상자원 관리시스템 로그인 계정 생성 시 비밀번호 규칙을 수립하여 적용하여야 한다.

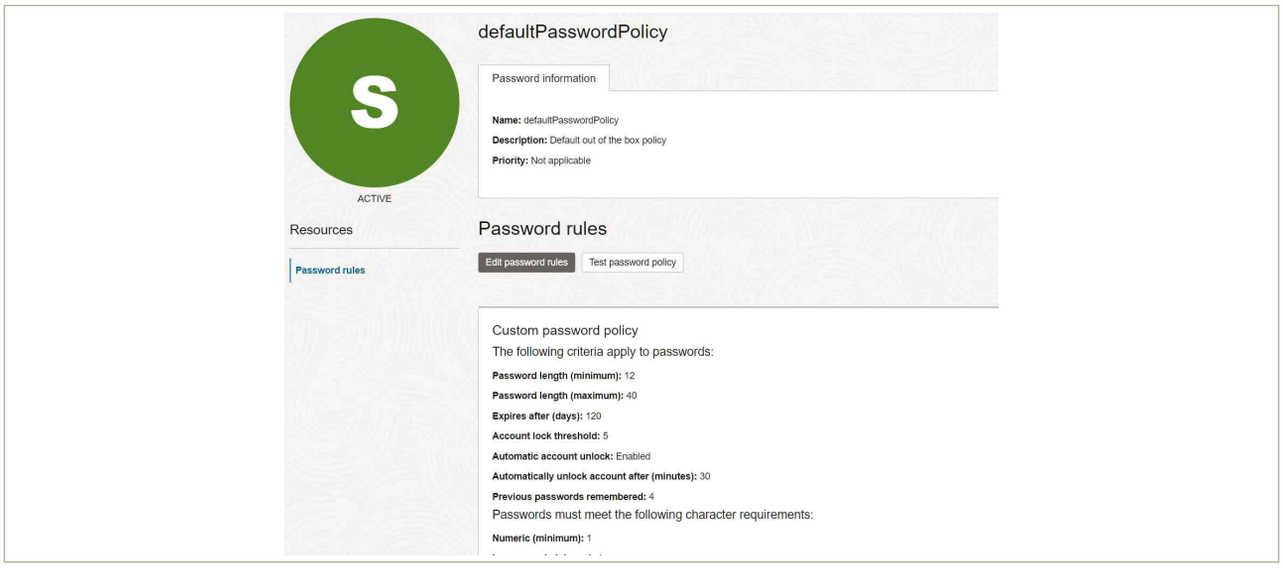
2 설명

- 클라우드 가상자원 관리시스템 접근 가능한 계정 생성 시 안전한 비밀번호 규칙을 수립하여 적용하여야 한다.

  1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

3 우수 사례

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Domain' → '도메인 선택' → 'Setting' → 'Password policy' → '생성한 패스워드 정책' → 'Edit password rules'에서 비밀번호 생성 규칙 수립 가능



| 그림 3.6.1 | 이용자 비밀번호 생성 규칙

4 참고 사항

- https://cloud.oracle.com/identity/domains/overview?region=ap-seoul-1

1 기준

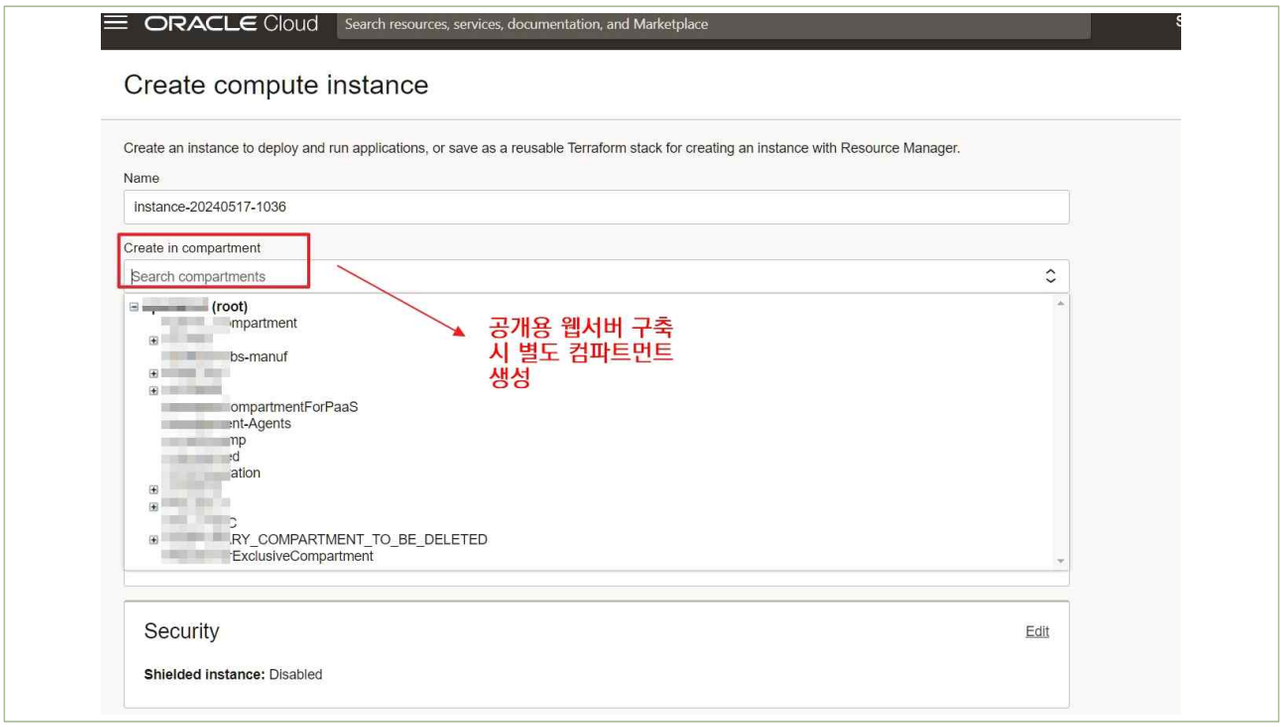
식별번호	기준	내용
3.7	**공개용 웹 서버 접근 계정 제한**	클라우드를 통해 공개용 웹 서버를 운영하는 경우 접근 계정을 적절하게 제한하여야 한다.

2 설명

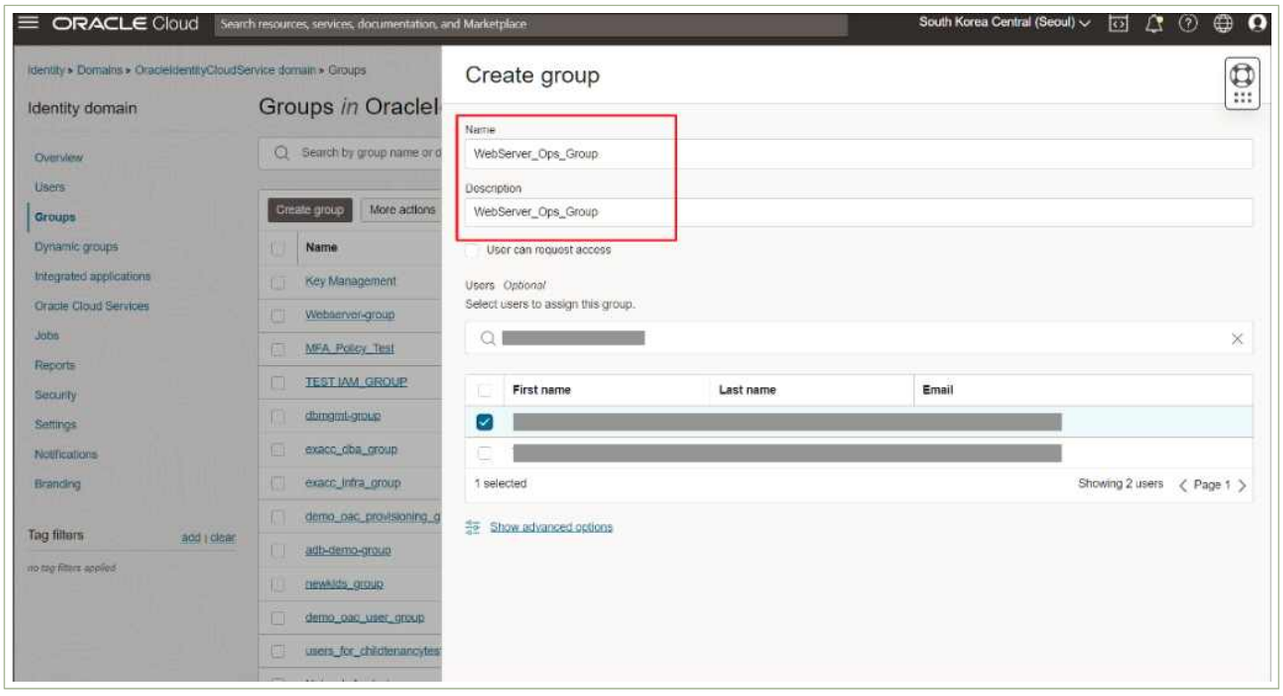
- 클라우드 환경을 통해 공개용 웹 서버를 운영하는 경우 접근 계정을 적절하게 제한하여야 한다.
  1) 계정 관리 기능을 통해 공개용 웹 서버만 접근 가능한 계정을 개인별 부여하여 관리
  2) 공개용 웹 서버에 접근 가능한 계정으로 로그인 시 추가인증 수단 적용 등

3 우수 사례

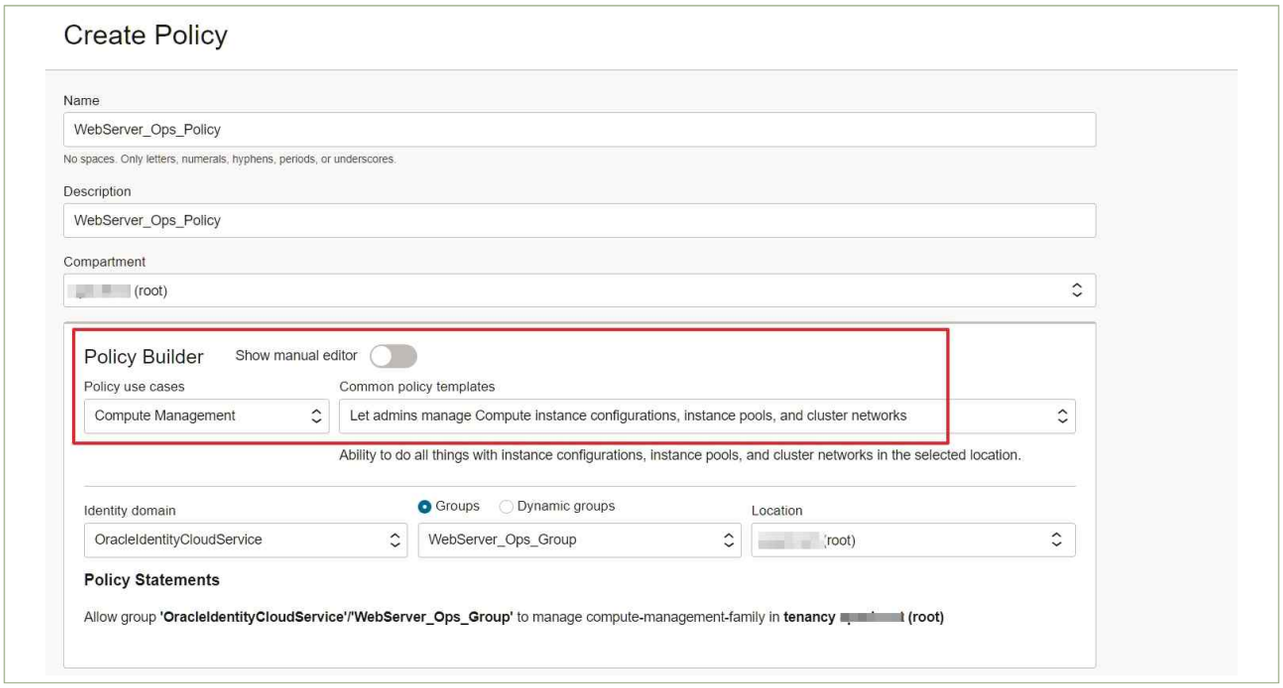
- (OCI 콘솔) '홈' → 'Compute' → 'Instances'에서 공개용 웹 서버 인스턴스를 위한 컴파트먼트(Compartment)를 생성하고, 이후 해당 컴파트먼트에 인스턴스를 생성



| 그림 3.7.1. | 공개용 웹 서버 생성



| 그림 3.7.2 | 웹 서버 관리자를 위한 그룹 및 사용자 지정



| 그림 3.7.3 | 웹 서버 접근 정책 설정

- 공개용 웹 서버를 관리하는 사용자(그룹)이 해당 컴파트먼트(Compartment)에서 권한을 가지도록 정책을 설정

4 참고 사항

- [정책 및 권한 할당]
  https://cloud.oracle.com/identity/domains/policies?region=ap-seoul-1

4. 암호 키 관리

4.1. 암호화 적용 가능 여부 확인
4.2. 암호 키 관리 방안 수립
4.3. 암호 키 서비스 관리자 권한 통제
4.4. 암호 키 호출 권한 관리
4.5. 안전한 암호화 알고리즘 적용

4 암호 키 관리

1 기준

식별번호	기준	내용
4.1	**암호화 적용 가능 여부 확인**	관련 법령(전자금융거래법, 신용정보법 등)에 따른 암호화 대상이 저장 및 처리되는 가상자원(서버, 스토리지 등)에 대한 암호화 기능 적용 여부를 확인하여야 한다.

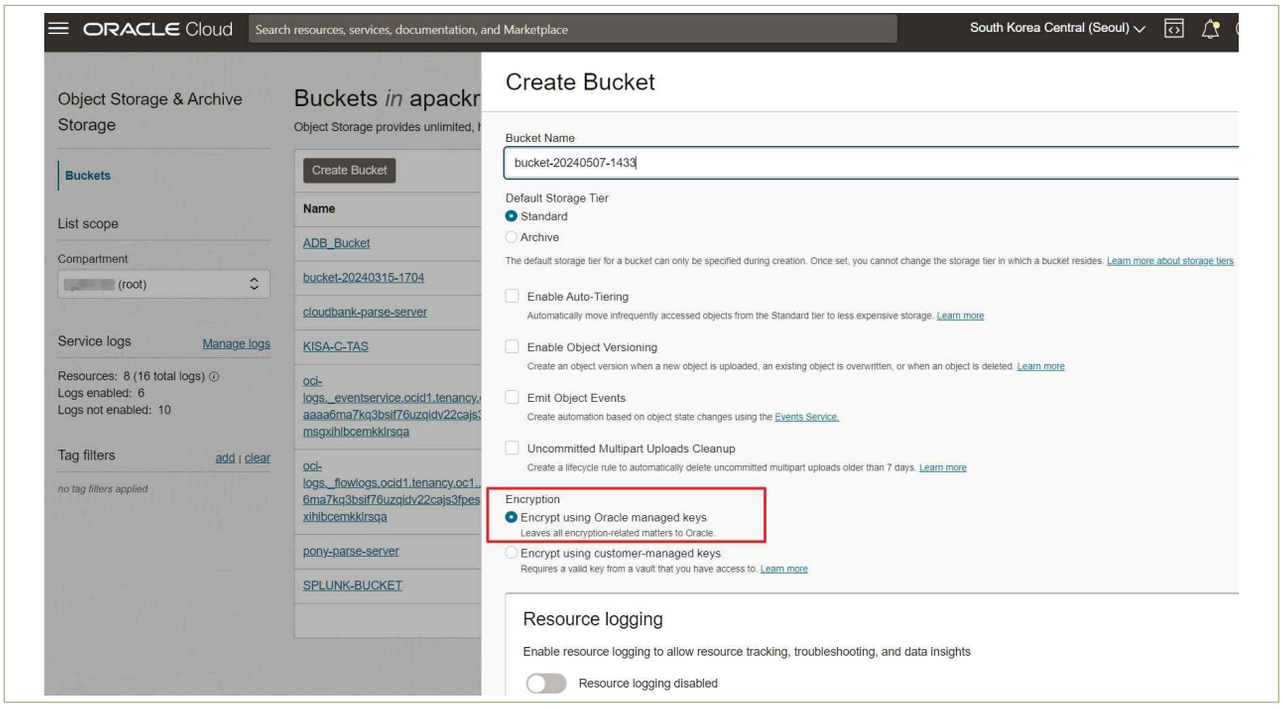
2 설명

- 관련 법령(전자금융거래법, 개인정보보호법, 신용정보법 등)에 따라 암호화가 필요한 대상이 저장 및 처리되는 가상자원에 대해서는 암호화 적용을 고려하여야 한다.
  1) 클라우드의 키 관리 서비스를 통해 CSP 사업자의 관리형 Key로 암호화
  2) 클라우드의 키 관리 서비스를 통해 이용자 관리형 Key 암호화
  3) 이용자가 직접 관리하는 Key로 암호화 등

3 우수 사례

1) 클라우드의 키 관리 서비스를 통해 CSP 사업자의 관리형 Key로 암호화

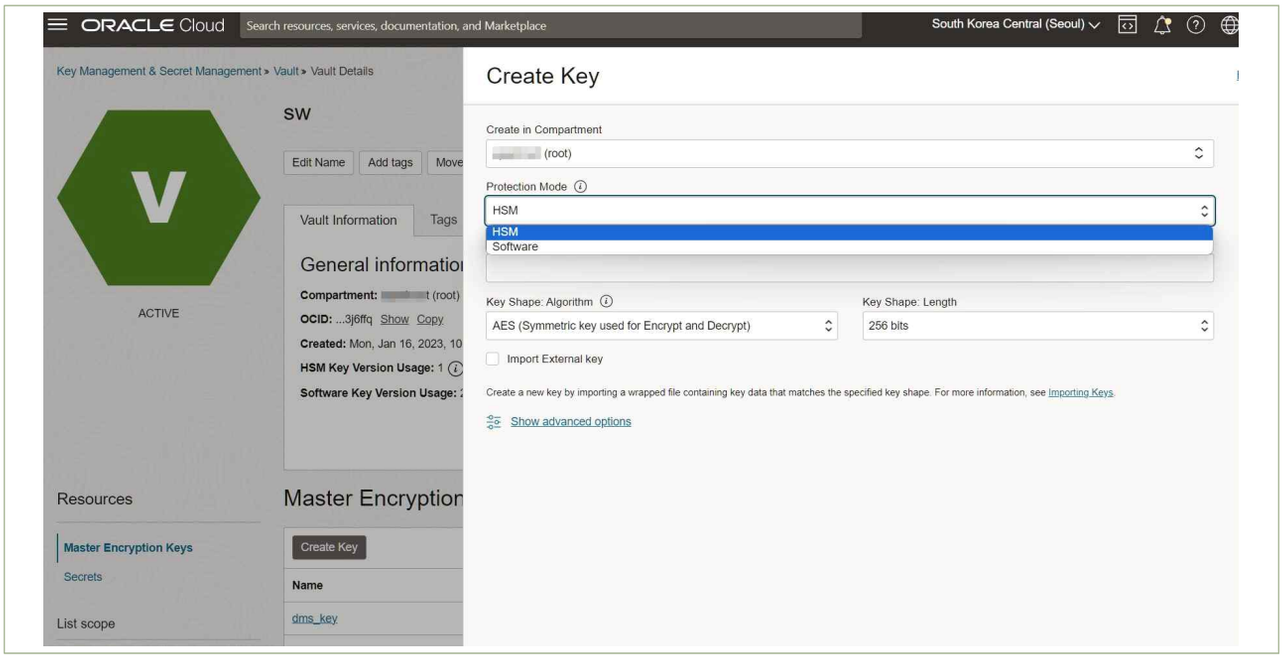
- (OCI 콘솔) ‘홈’ → ‘Storage’ → ‘Object Storage & Archive Storage’ → ‘Buckets’ → ‘Create Bucket’을 선택한 후, '오라클 관리형 키(Encryption using Oracle managed keys)'를 지정하여 CSP 사업자의 관리형 키로 데이터를 암호화



| 그림 4.1.1 | Oracle managed key를 통한 암호화

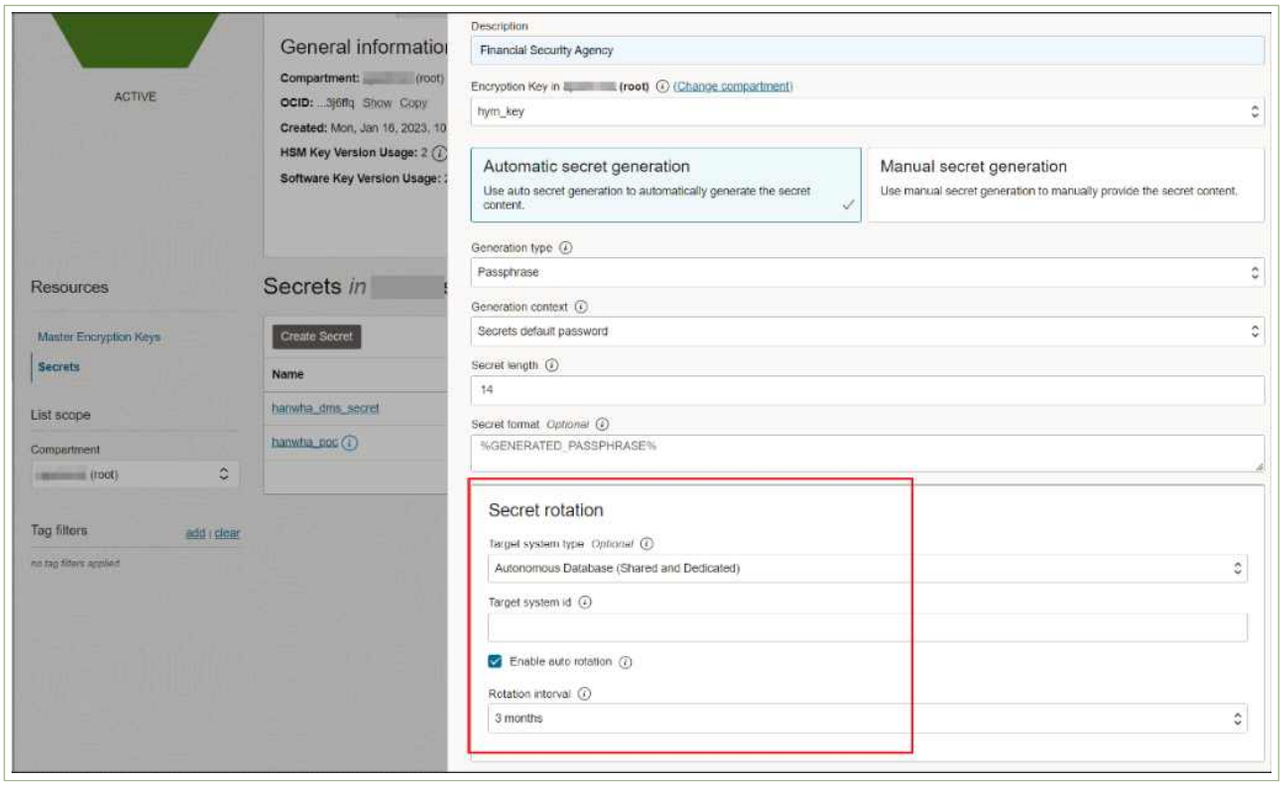
2) 클라우드의 키 관리 서비스를 통해 이용자 관리형 Key 암호화

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Key Management & Secret Management' → 'Vault'에서 최초 마스터 키를 생성할 수 있으며, 이때 키 보호를 위한 하드웨어/소프트웨어, 암호화 알고리즘, 키 길이 선택 옵션 제공



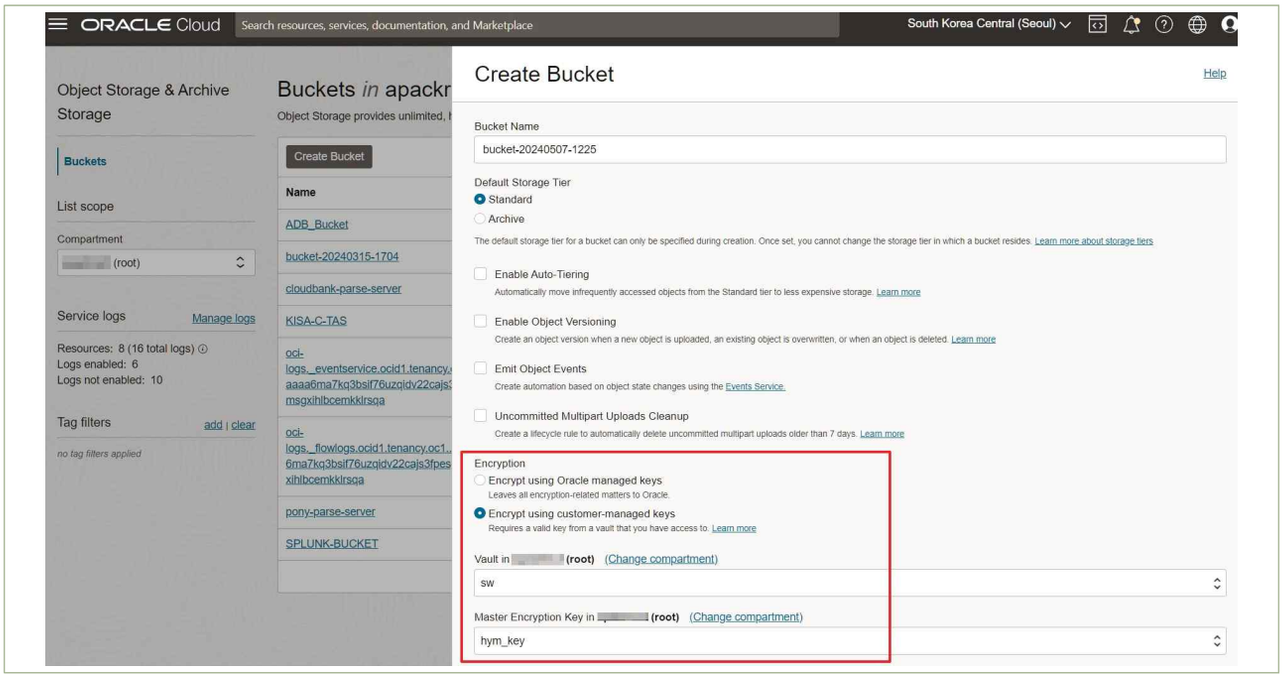
| 그림 4.1.2 | Key Management를 통한 Master key 생성

- 관리형 키를 활용하여 Autonomous Database, OCI Function 데이터 암호화



| 그림 4.1.3 | Secret rotation 설정

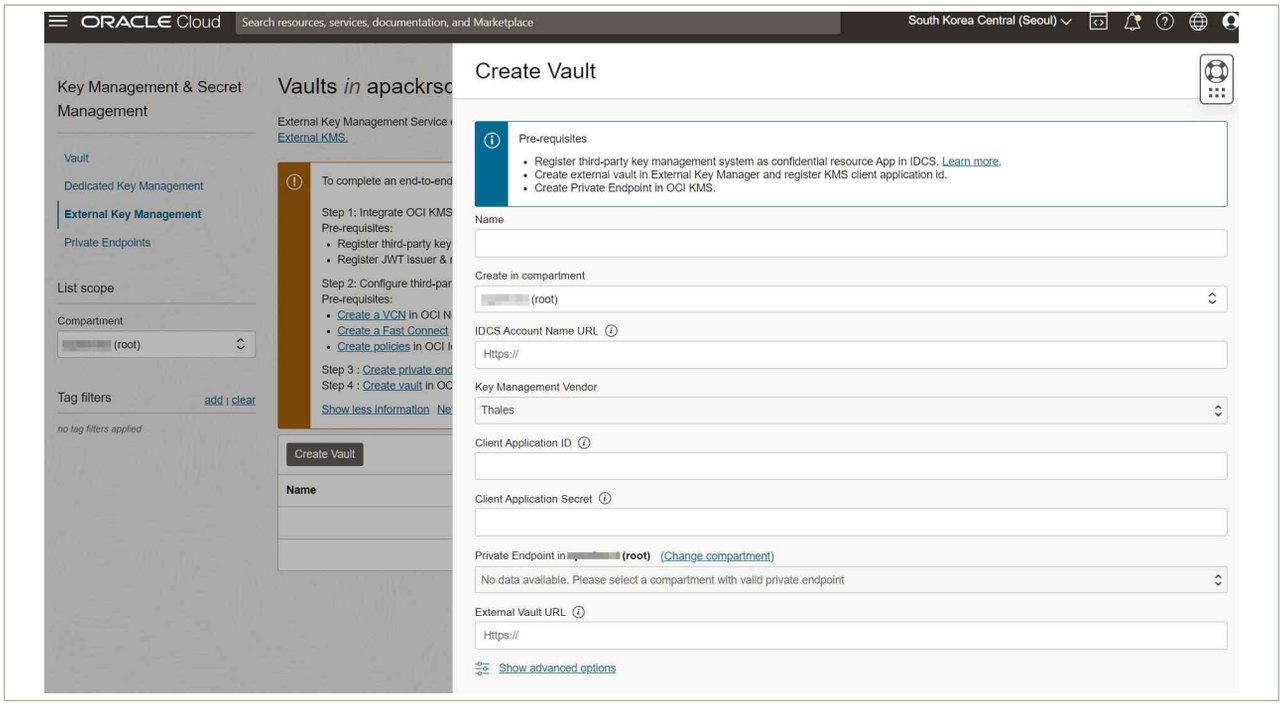
- 관리형 키를 활용하여 Object storage 데이터 암호화



| 그림 4.1.4 | 관리형 키를 활용하여 Bucket 암호화

3) 이용자가 직접 관리하는 Key로 암호화 등

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Key Management & Secret Management' → 'External Key Management' → 'Create Vault'에서 이용자가 외부에서 관리되는 키를 직접 활용할 수 있도록 지원



| 그림 4.1.5 | 외부 키 관리(External Key Management)

4 참고 사항

- [버킷 생성 시 암호화]
  https://cloud.oracle.com/object-storage/buckets?region=ap-seoul-1
- [Key Management & Secret Management]
  https://cloud.oracle.com/security/kms?region=ap-seoul-1
- [External Key Management]
  https://cloud.oracle.com/security/external-hsm?region=ap-seoul-1

1 기준

식별번호	기준	내용
4.2	**암호 키 관리 방안 수립**	암호화 기능 이용 시 암호 키 관리방안을 수립하여야 한다.

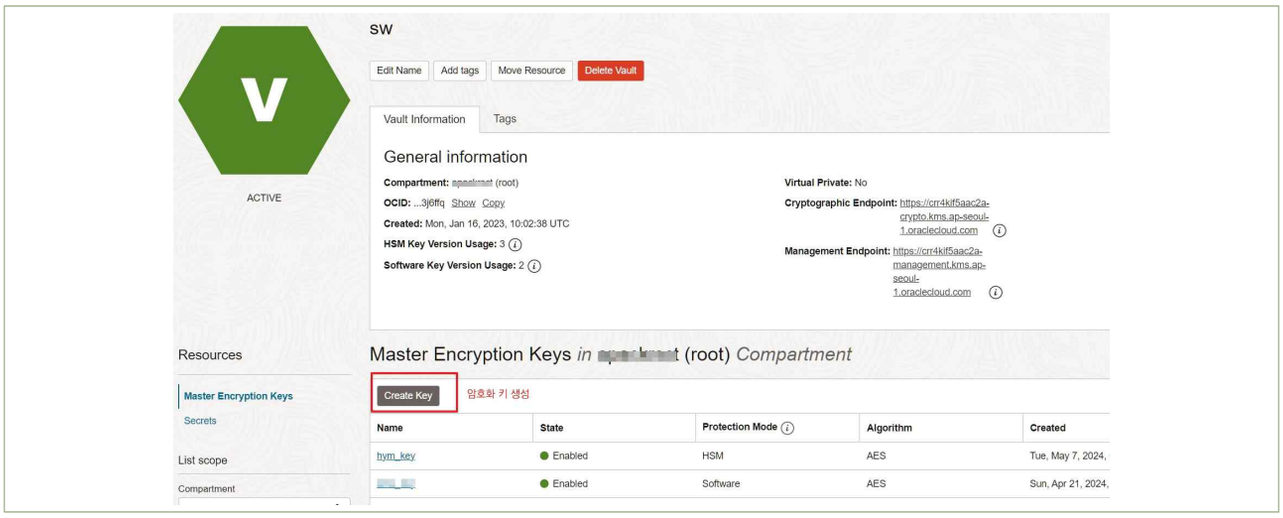
2 설명

- 암호화 기능 이용 시 암호 키 관리 방안을 수립하여야 한다.
  1) KMS(Key Management Service)를 통한 암호화 키 방안 수립(생성, 변경, 폐기 등)
  2) 클라우드 서비스 제공자가 직접 제공하는 암호화키 이용 시 적절한 관리방안 수립
  3) 키 사용기간 수립 및 암호 키 유출 등에 대응할 수 있도록 키 삭제 및 재적용 관련 기능 수립
  4) 생성한 암호화키를 안전하게 보관할 수 있는 방안 수립 등

3 우수 사례

1) KMS(Key Management Service)를 통한 암호화 키 관리 방안 수립(생성, 변경, 폐기 등)

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Key Management & Secret Management' → 'Vault' → 'Vault Details'에서 암호화 키 생성, 변경(Rotate), 폐기할 수 있도록 지원

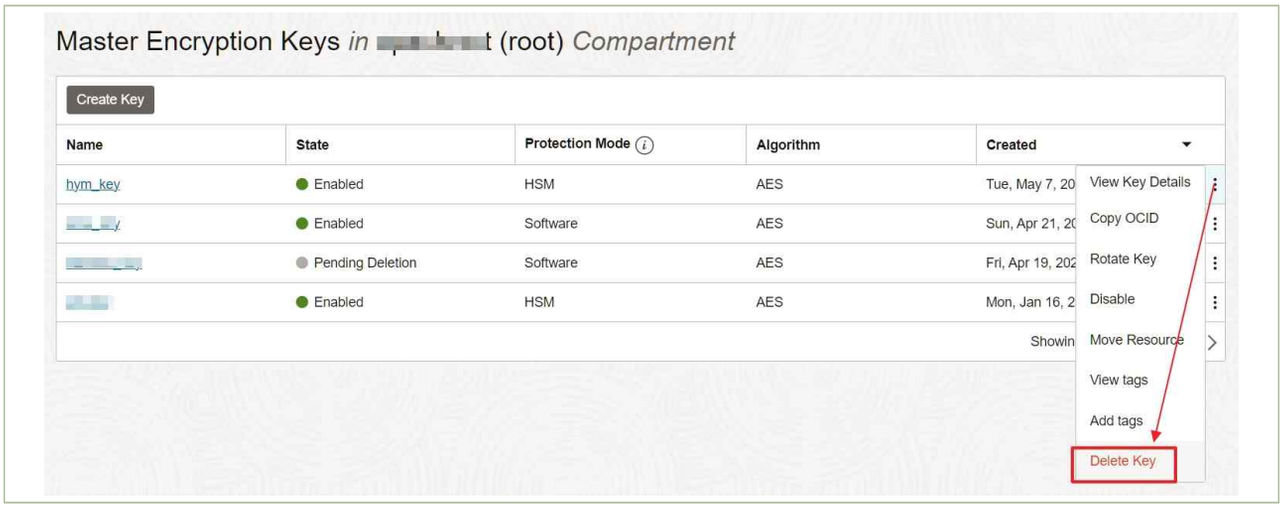


| 그림 4.2.1 | 암호화 키 생성

- 내부 보안 규정에 따라 암호화 키의 수명 주기를 고려해 키 교체(Rotate)를 권장

| 그림 4.2.2 | 암호화 키 변경(Rotate)

- 사용 목적이 완료되었거나 사용하지 않는 키를 정기적으로 검토하고, 필요에 따라 암호화 키를 삭제해야 함



| 그림 4.2.3 | 암호화 키 삭제

2) 클라우드 서비스 제공자가 직접 제공하는 암호화 키 이용 시 적절한 관리 방안 수립

- 아래 5가지 방법으로 오라클 클라우드가 제공하는 암호화 키 이용 시 관리 방안 기준 및 보호 대책 제공

① 키 생성 및 관리 정책 수립

[키 생성] 중요한 데이터와 시스템을 보호할 수 있도록 강력한 암호화 알고리즘을 사용(AES-256등 강력한 알고리즘 지원)

[키 생명 주기 관리] 키의 생성, 활성화, 비활성화, 폐기 등 키의 전체 수명 주기를 정의하고 관리

② 키 접근 제어

[정책 설정] OCI 콘솔에서 키 관리와 관련된 IAM 정책을 설정 (예를 들어 특정 그룹이나 사용자만 키를 생성하고 관리할 수 있도록 제한)

③ 키 사용 모니터링 및 로깅

[감사 로그(Audit Logs)] OCI Audit 서비스를 사용하여 키의 사용 이력을 기록하고 모니터링(키의 생성, 접근, 사용, 삭제 등의 모든 활동을 로그로 남김)

[이벤트 알림] OCI 이벤트(Event) 서비스의 알림(Notification) 서비스를 연계해 키와 관련된 중요한 이벤트 발생 시 알림. 예를 들어, 키의 비정상적인 접근 시도를 모니터링하고 알림을 받을 수 있음

④ 데이터 암호화

[데이터 암호화 적용] OCI 키 관리(Key Management) 서비스에서 생성한 키를 사용하여 저장 데이터와 전송 데이터를 암호화

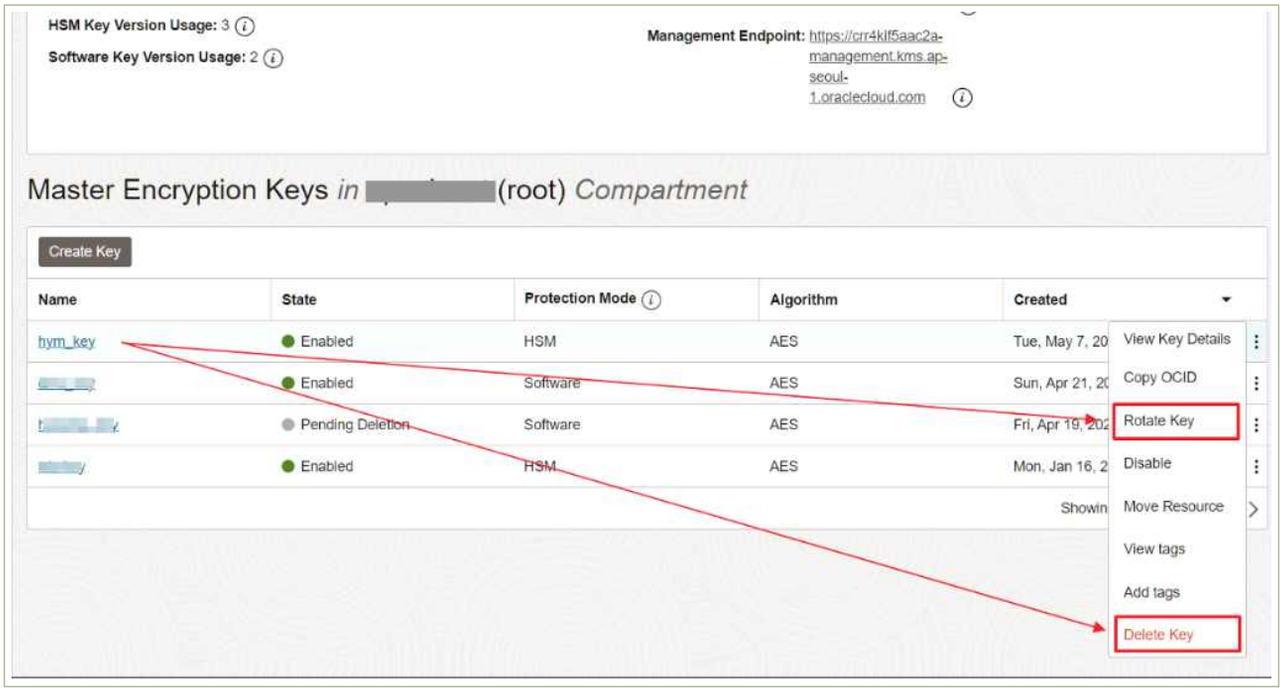
[연계 서비스 사용] 오라클 데이터베이스, 블록 스토리지, 오브젝트 스토리지 등 OCI 서비스에서 제공하는 기본 암호화 기능을 사용

⑤ 보안정책 및 규정준수

[규정 준수] HIPAA, GDPR, PCI-DSS 등과 같은 산업 규정을 준수하기 위해 필요한 키 관리 절차를 설정 (규정 준수 요구사항에 따라 키의 보관 위치, 접근 제어, 감사 요구사항 등을 관리)

3) 키 사용 기간 설정 및 암호 키 유출 등에 대응할 수 있도록 키 삭제 및 재적용 관련 기능 구축

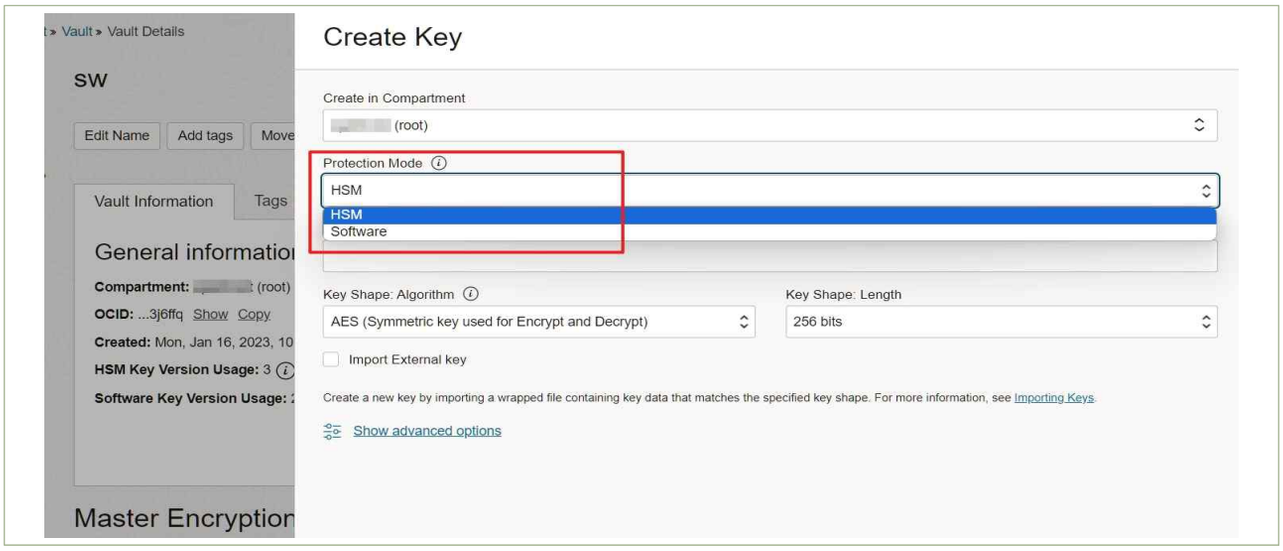
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Key Management & Secret Management' → 'Vault' → 'Vaults in (root) Compartment' → '적용할 키 선택' 오른쪽 메뉴 버튼을 클릭하여 키 삭제 및 재적용을 위한 키를 로테이션 할 수 있도록 지원



| 그림 4.2.4 | 생성한 키 삭제 및 키 변경

4) 생성한 암호화 키를 안전하게 보관할 수 있는 방안 수립 등

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Key Management & Secret Management' → 'Vault'에서 암호화 키를 안전하게 보관할 수 있는 Protection mode 제공
  - 암호화 대상 시스템(Database, Object storage 등)과 내부 규정에 따라 필요한 Protection mode를 선택하여 암호 키를 보관할 수 있도록 지원



| 그림 4.2.5 | 암호 키 Protection mode

4 참고 사항

- [Key Management & Secret Management]
  https://cloud.oracle.com/security/kms?region=ap-seoul-1

1 기준

식별번호	기준	내용
4.3	**암호 키 서비스 관리자 권한 통제**	클라우드 암호 키 서비스 이용 시 관리자 권한은 최소인원에게 부여하고 모니터링 하여야 한다.

2 설명

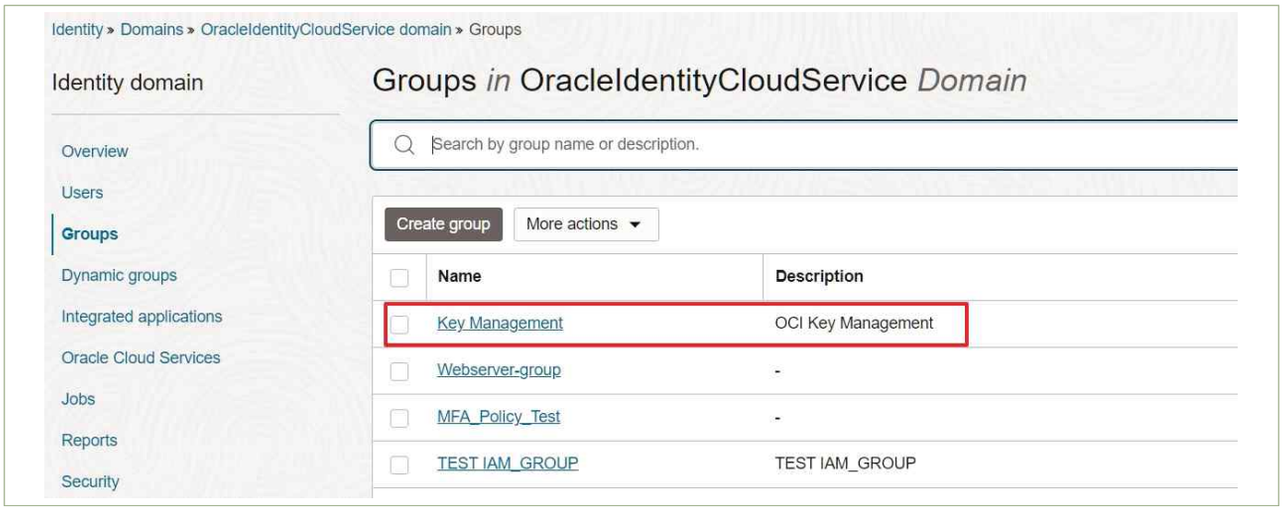
- 클라우드 환경 내 암호 키 관리 서비스(ex. KMS) 이용 시 암호 키 서비스 관리자 권한을 적절하게 통제하여야 한다.
  1) 암호 키 관리 서비스 관리자 권한은 최소인원에게 부여하고 부여 현황에 대해 상시 모니터링 수행
  2) 사용자가 생성하는 각 키에 대해서는 관리자를 별도 지정할 수 있어야 하며, 각 조건에 따라 최소한의 권한 부여 등

3 우수 사례

1) 암호 키 관리 서비스 관리자 권한은 최소 인원에게만 부여하고, 부여 현황에 대해 상시 모니터링 수행

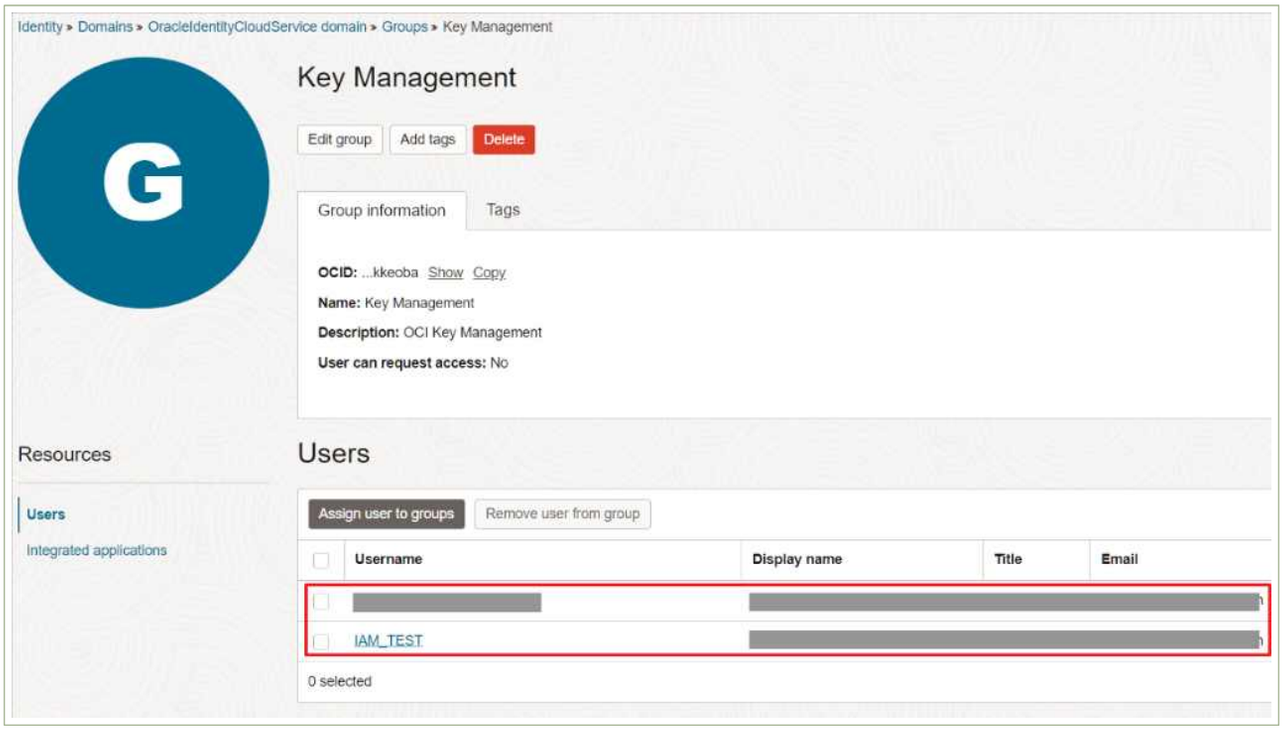
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Domain' → 'Default Domain' → 'Groups' → 'Create Group'에서 암호화 키 관리 서비스 관리자를 최소 인원으로 구성
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' → 'Create Policy'에서 Policy builder를 통해 Policy use case, Common policy templates를 사용하여 최소 인원에게 암호화 키 관리 서비스의 관리자 권한을 지정할 수 있음

- 암호화 키 관리자 지정을 위한 사용자 그룹 생성

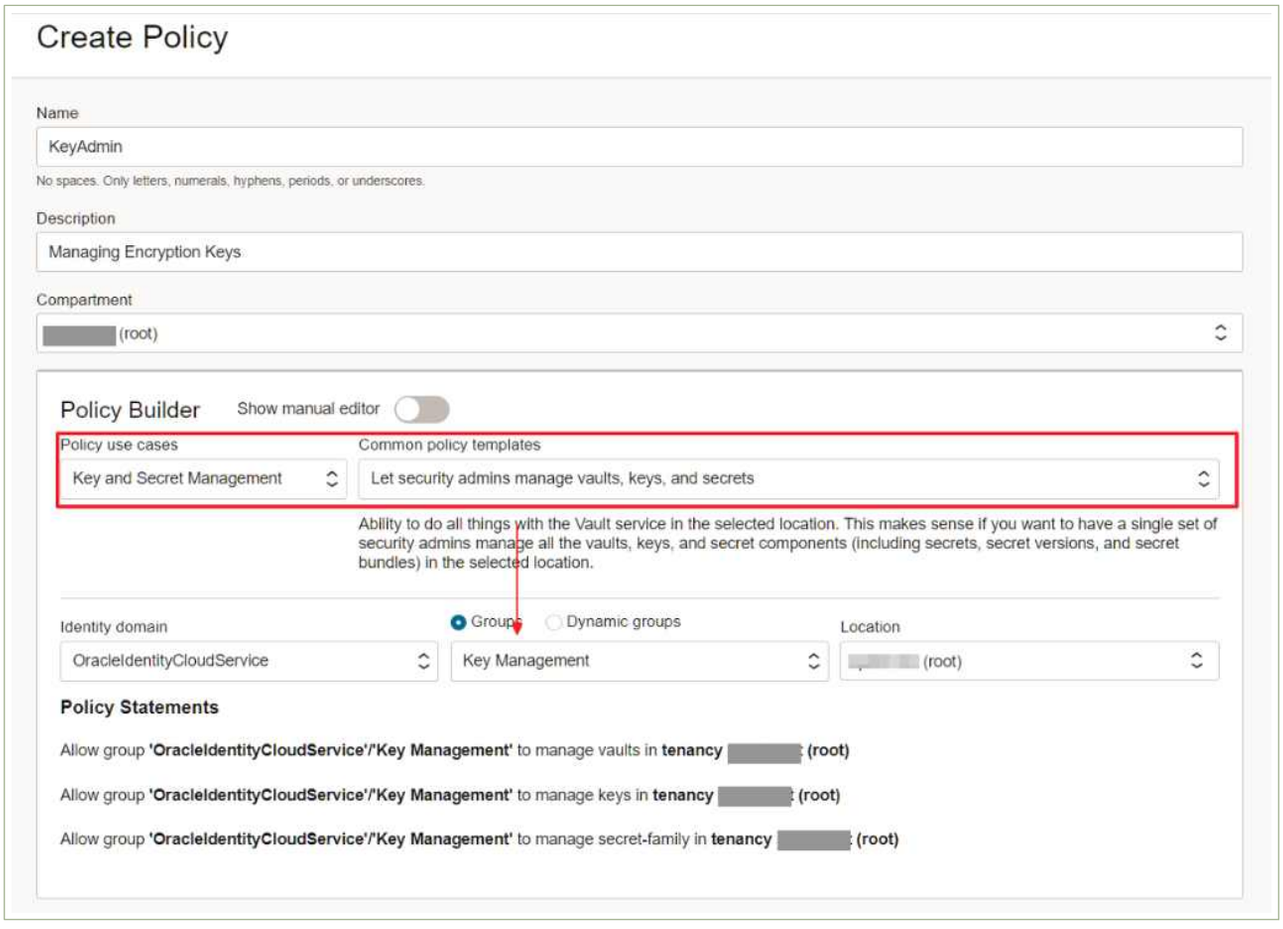


| 그림 4.3.1 | 암호화 키 관리 서비스 관리자 권한 설정

- 보안 관리자가 Vault, Key, Secrets을 관리할 수 있도록 허용



| 그림 4.3.2 | Policy Builder 관리자 권한 지정



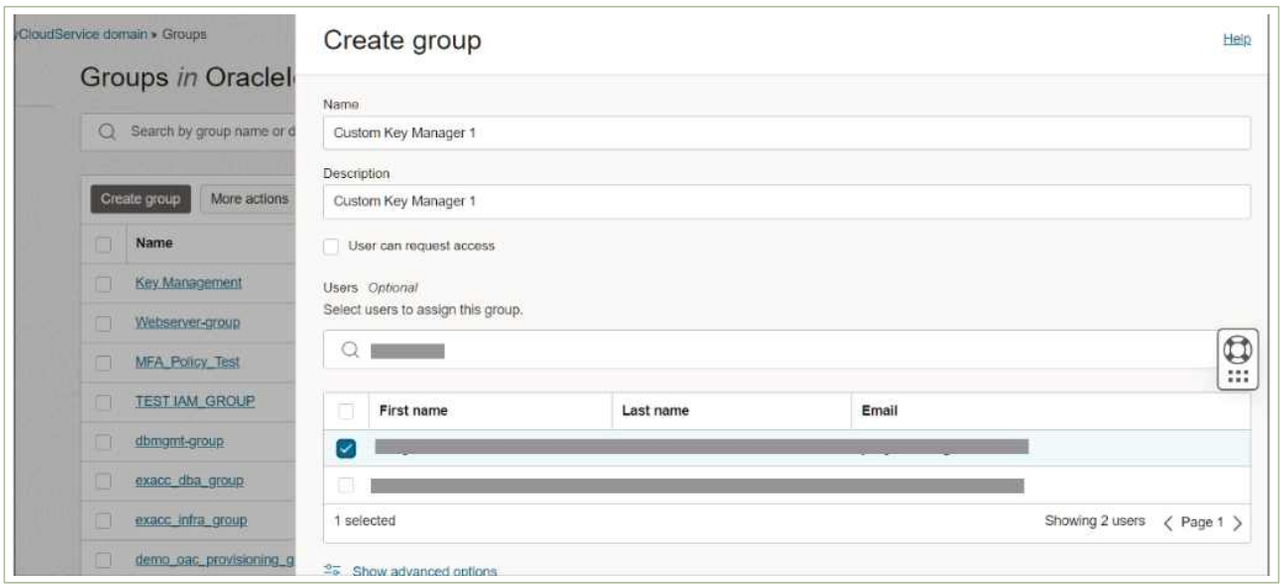
| 그림 4.3.3 | Policy Builder 관리자 권한 지정

- 암호화 키 관리자에게 권한 할당이 완료됨

| 그림 4.3.4 | Key 관리자 권한할당 화면

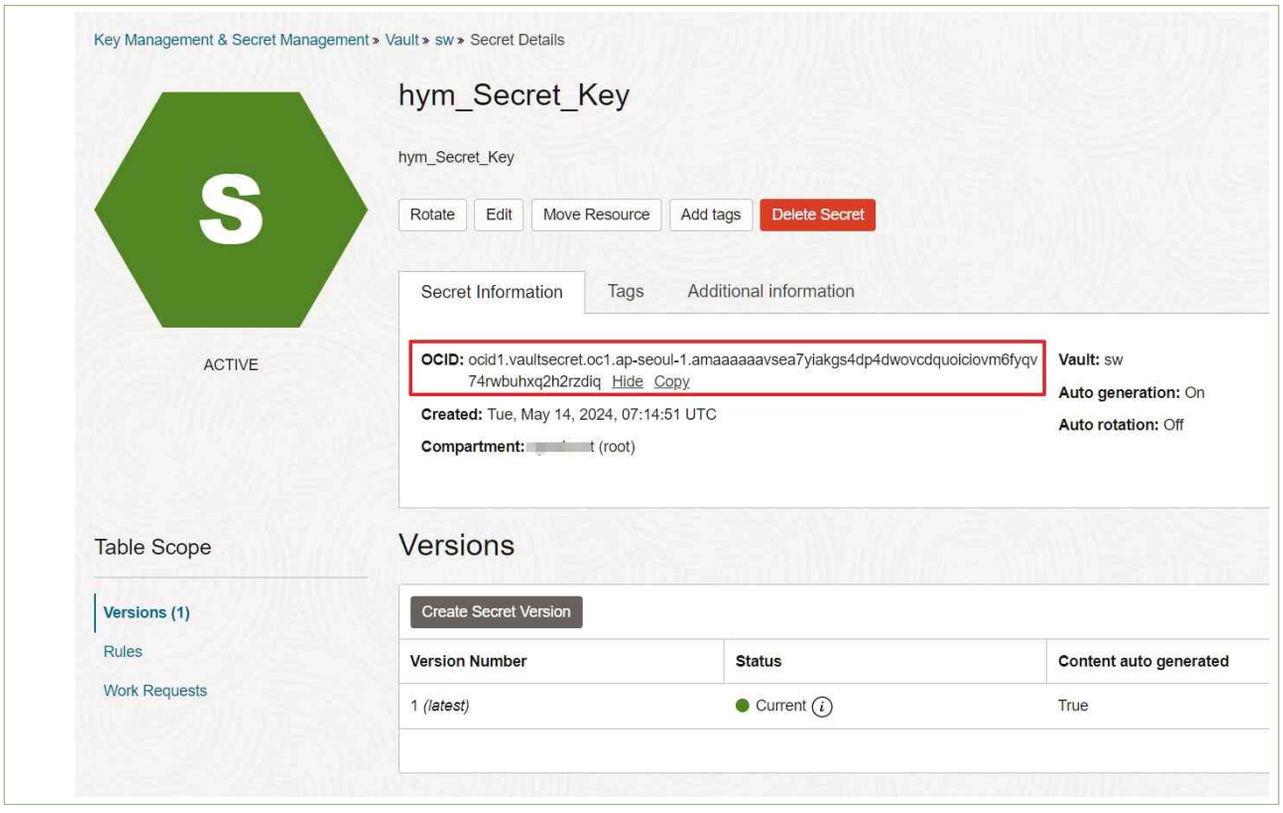
2) 사용자가 생성하는 각 키에는 별도 관리자를 지정할 수 있어야 하며, 각 조건에 따라 최소한의 권한 부여 등

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Domain' → 'Default Domain' → 'Groups' → 'Create Group'에서 암호화 키별 그룹을 생성
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' → 'Create Policy'에서 Policy builder를 통해 사용자가 생성한 각 키(OCID)에 대해 사용자 그룹을 지정하고, 키 마다 관리자를 지정하도록 지원
  - 사용자가 생성한 암호화 키마다 관리 정책을 할당하기 위해 그룹을 생성(Custom Key Manager 1…n)



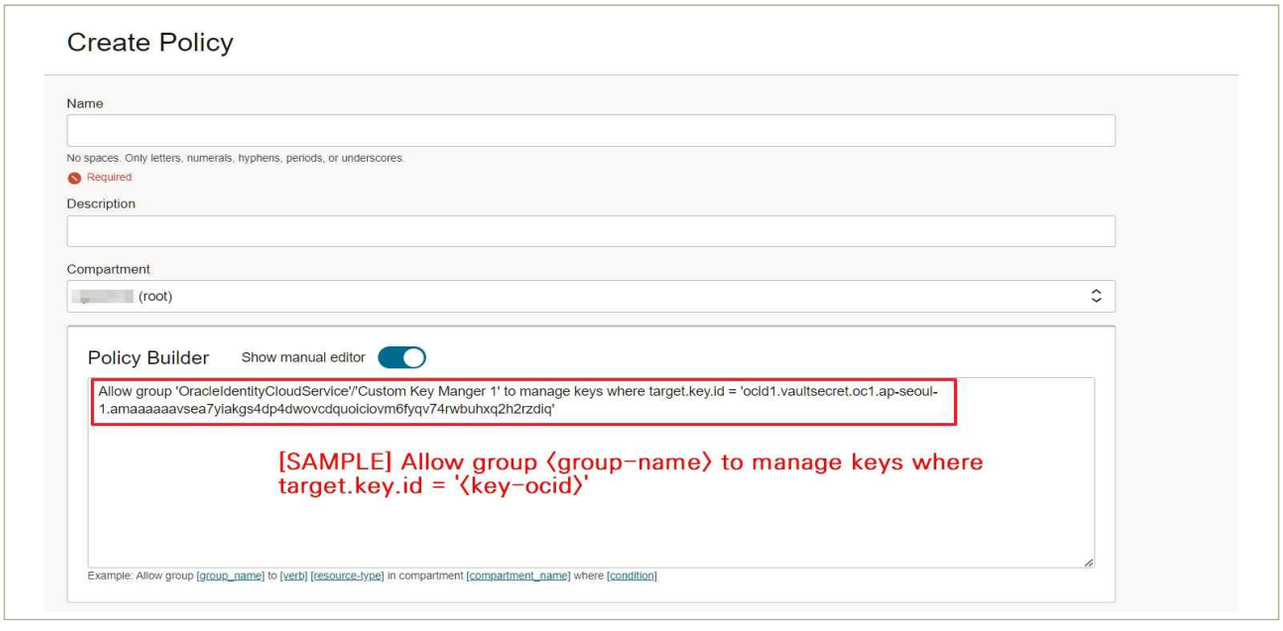
| 그림 4.3.5 | 암호 키 관리 서비스 관리자 권한 설정

- 사용자가 생성한 각 암호화 키에 대한 권한을 할당하기 위해 사전에 키의 OCID 값 확인



| 그림 4.3.6 | 사용자 생성한 암호 키 OCID 값 확인

- 보안 관리자가 Vault, Key, Secrets을 관리하도록 허용



| 그림 4.3.7 | Policy Builder 관리자 권한 지정

4 참고 사항

- [Identity]
  https://cloud.oracle.com/identity/domains/overview?region=ap-seoul-1
- [정책 및 권한할당]
  https://cloud.oracle.com/identity/domains/policies?region=ap-seoul-1

1 기준

식별번호	기준	내용
4.4	**암호 키 호출 권한 관리**	클라우드 암호 키 호출 권한을 관리하여야 한다.

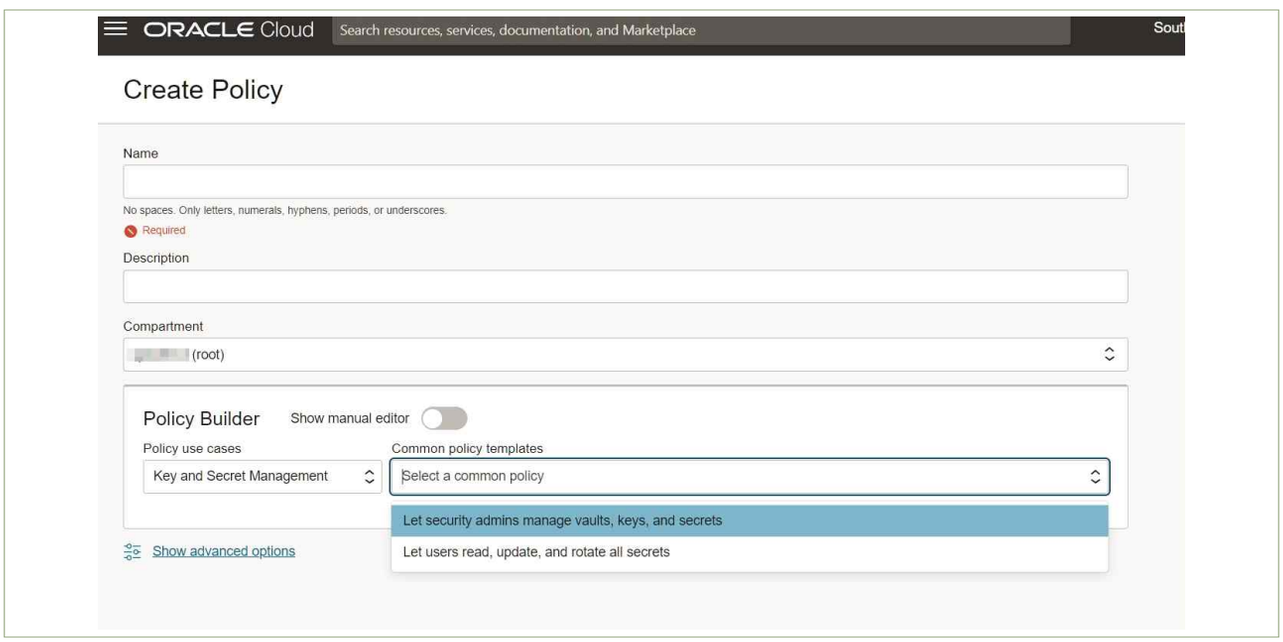
2 설명

- 클라우드 암호 키 호출에 관한 사항(암호화, 복호화, 암호 키 변경, 삭제 등)은 이용자의 권한 및 업무에 따라 적절하게 부여하고 관리하여야 한다.
  1) 암호 키 관리서비스(KMS)를 통해 암호 키 호출 시 목적에 따라 권한 부여
  2) 암호 키 호출 권한 현황에 대한 모니터링 및 주기적 검토 수행

3 우수 사례

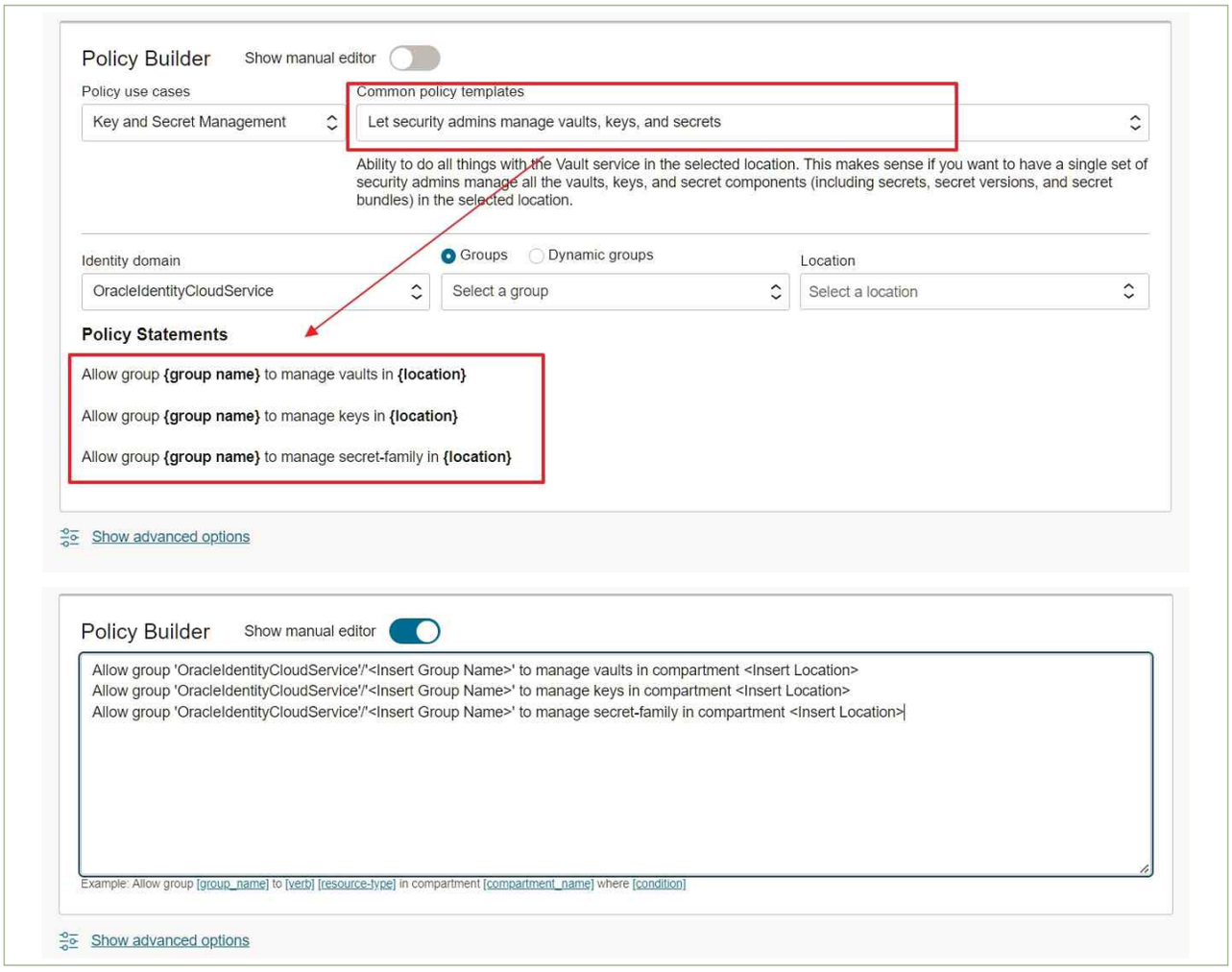
1) 암호화 키 관리 서비스(KMS)를 통해 암호화 키 호출 시 목적에 따라 권한 부여

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' → 'Create Policy'에서 암호화 키 호출 목적에 따라 권한을 세부적으로 설정 가능



| 그림 4.4.1 | 암호화 키 권한 세부 설정을 위한 정책 생성

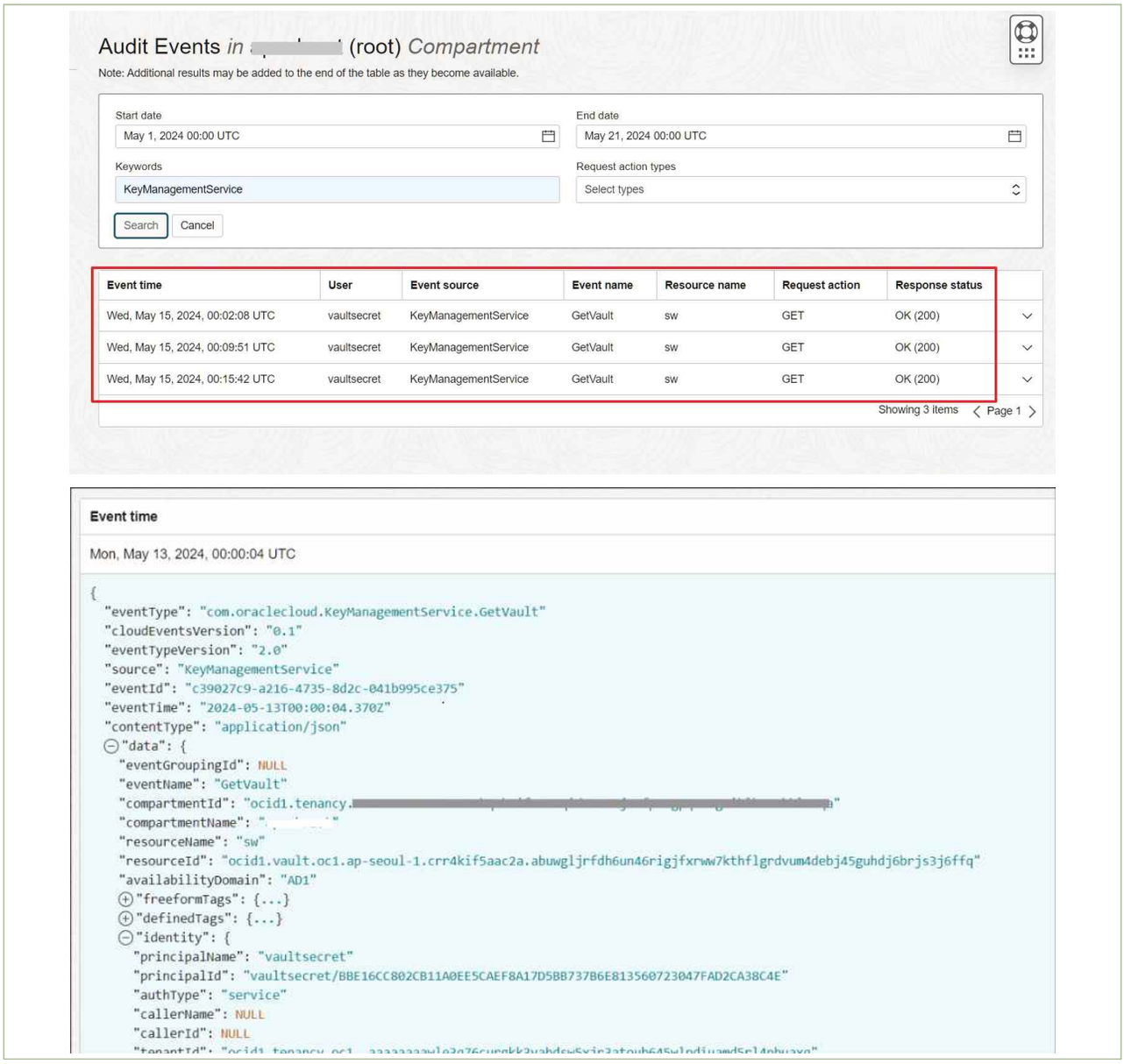
- 'Key and Secret Management'에서 암호화 키 호출에 관한 권한 부여 템플릿을 선택하여 정책을 자동으로 생성



| 그림 4.4.2 | 암호화 키 호출 권한 템플릿 선택

2) 암호화 키 호출 권한 현황에 대한 모니터링 및 주기적 검토 수행

- (OCI 콘솔) '홈' → 'Observability & Management' → 'Logging' → 'Audit'에서 암호화 키('KeyManagementService') 호출 권한 현황을 모니터링



| 그림 4.4.3 | 암호화 키 호출 모니터링

4 참고 사항

- [정책 및 권한 할당]
  https://cloud.oracle.com/identity/domains/policies?region=ap-seoul-1

1 기준

식별번호	기준	내용
4.5	**안전한 암호화 알고리즘 적용**	암호화 기능 이용 시 안전한 암호화 알고리즘을 적용하여야 한다.

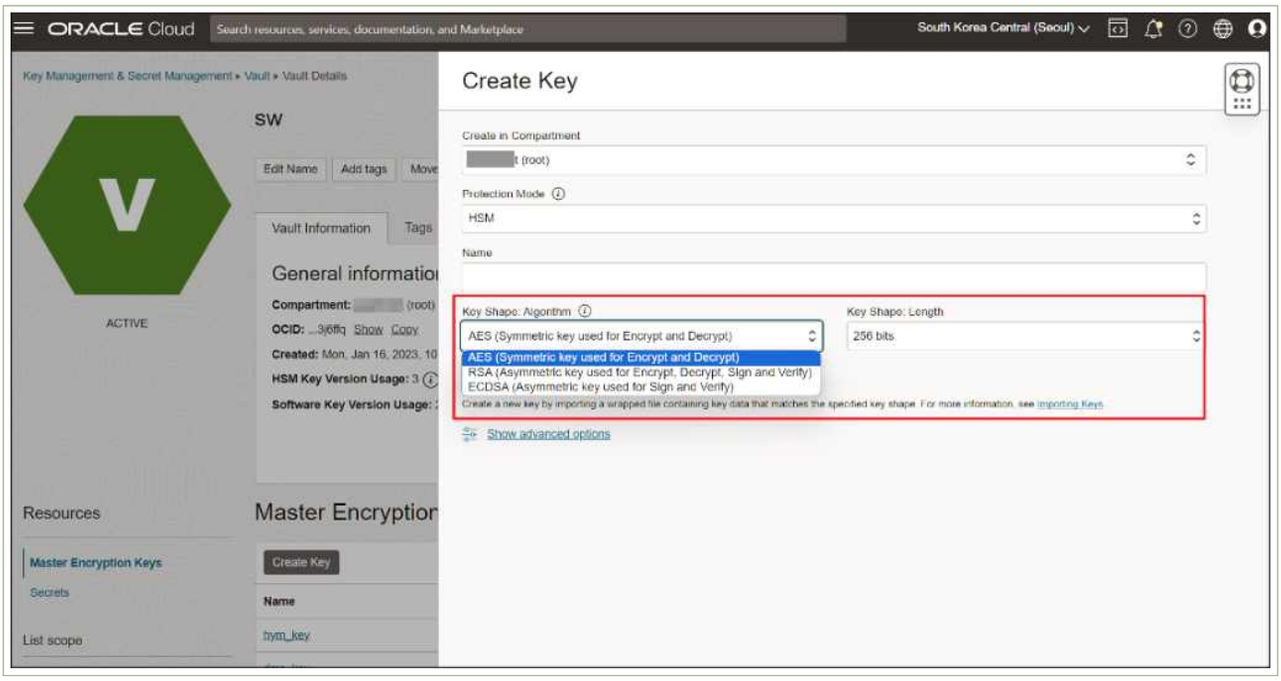
2 설명

- 암호화 기능 이용 시 안전한 암호화 알고리즘을 적용하여야 한다.
  1) 이용자가 관리하는 암호화 키로 암호화 기능 적용 시 안전한 암호화 알고리즘 적용
  2) 클라우드 KMS 서비스를 통해 암호화 시 안전한 암호화 알고리즘을 제공하는지 확인

3 우수 사례

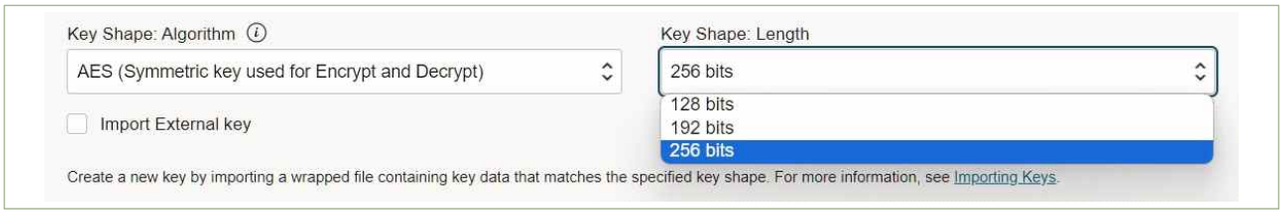
1) 이용자가 관리하는 암호화 키로 암호화 기능 적용 시 안전한 암호화 알고리즘 적용(금융부문 암호기술 활용 가이드 참고)

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Key Management & Secret Management' → 'Vault' → 'Create Key'



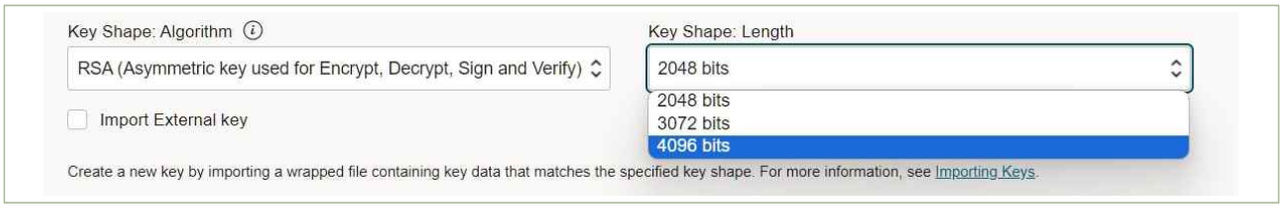
| 그림 4.5.1 | 암호 알고리즘 종류 및 암호 강도

- 대칭키 암호화 알고리즘 (KISA 권고사항인 128bit이상~256bit이상 모두 지원)



| 그림 4.5.2 | 대칭키 길이 화면

- 공개 키 암호 알고리즘 (KISA 권고사항인 112bit~128bit이상을 지원)
- 공개 키 암호 알고리즘 보안 강도(공개 키) : 112:2048, 128:3072, 192:7680



| 그림 4.5.3 | 공개키 길이 화면

- 국내외 권고 암호 알고리즘

분류		NIST(미국) (2015)	CRYPTREC(일본) (2013)	ECRYPT(유럽) (2018)	국내[1] (2018)
대칭키 암호 알고리즘 (블록암호)		AES 3TDEA[2]	AES Camellia	AES Camellia Serpent	SEED HIGHT ARIA LEA
해시함수		SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512 SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHA3-shake128[3] SHA3-shake256[3] Whirlpool-512 BLAKE-256 BLAKE-384 BLAKE-512	SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 LSH-224 LSH-256 LSH-384 LSH-512 LSH-512-224 LSH-512-256
공개키 암호 알고리즘	키 공유용	DH ECDH MQV ECMQV	DH ECDH	ECIES-KEM PSEC-KEM RSA-KEM	DH ECDH
	암·복호화용	RSA	RSA-OAEP	RSA-OAEP	RSAES

보안강도	대칭키 암호 알고리즘 (보안강도)	해시함수 (보안강도)	공개키 암호 알고리즘				암호 알고리즘 안전성 유지기간 (년도)
			인수분해 (비트)	이산대수		타원곡선 암호(비트)	
				공개키(비트)	개인키(비트)		
112 비트	112	112	2048	2048	224	224	2011년에서 2030년까지
128 비트	128	128	3072	3072	256	256	2030년 이후
192 비트	192	192	7680	7680	384	384	
256 비트	256	256	15360	15360	512	512	

| 그림 4.5.4 | KISA 암호 알고리즘 및 키 길이 이용 안내서 - 2018

2) 클라우드 KMS 서비스의 안전한 암호화 알고리즘 제공 여부 확인

- OCI KMS는 AES, RSA, SHA와 같은 강력한 암호화 알고리즘을 제공하여 데이터를 안전하게 보호합니다. 이러한 알고리즘은 국제 표준을 준수하며, FIPS 인증을 받은 HSM에서 키를 관리하여 높은 수준의 보안을 보장
  - AES-256 : AES는 대칭 키 알고리즘으로, 동일한 키로 데이터를 암호화하고 복호화 하며, 256bit key를 사용하여 높은 보안 수준을 제공
  - RSA-2048(2048bit key), RSA-3072(3072bit key) : RSA는 비대칭 키 알고리즘으로, 공개키와 개인 키 쌍을 사용
  - SHA-256 : 256bit 해시 값을 생성하는 해시 알고리즘으로, 주로 데이터의 무결성 검증에 사용

4 참고 사항

- [Key Management & Secret Management]
  https://cloud.oracle.com/security/kms?region=ap-seoul-1
- [메뉴얼]
  https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm

5. 로깅 및 모니터링 관리

5.1. 가상자원 이용(생성, 삭제, 변경등)에 관한 행위추적성 확보
5.2. 가상자원 이용 행위추적성 증적 모니터링
5.3. 이용자 가상자원 모니터링 기능 확보
5.4. API 사용(호출대상, 호출자, 호출일시등)에 관한 행위추적성 확보
5.5. 네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보
5.6. 계정 변동 사항에 대한 행위추적성 확보
5.7. 계정 변경 사항에 관한 모니터링 수행

5 로깅 및 모니터링 관리

1 기준

식별번호	기준	내용
5.1	**가상 자원 이용(생성, 삭제, 변경 등)에 관한 행위 추적성 확보**	이용자의 가상 자원(서버, 데이터베이스, 스토리지 등) 이용 관련 행위추적성(로그 등)을 확보하여야 한다.

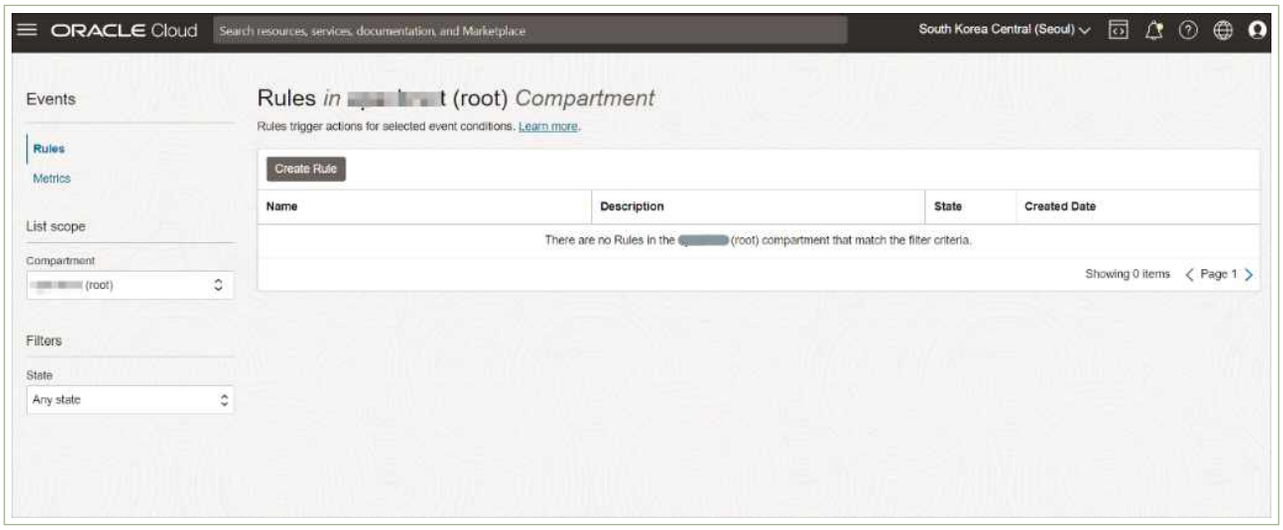
2 설명

- 이용자의 가상 자원 이용 관련 일련의 행위에 대한 추적성을 확보할 수 있는 방안이 마련되어야 한다.
  1) 가상 자원 변경 사항에 관한 행위(생성, 변경, 삭제 등)
  2) 가상 자원에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
  3) 가상 자원을 이용한 일시, 사용자 및 가상 자원의 형태(서버, 데이터베이스, 스토리지 등) 확인할 수 있는 접근기록

3 우수 사례

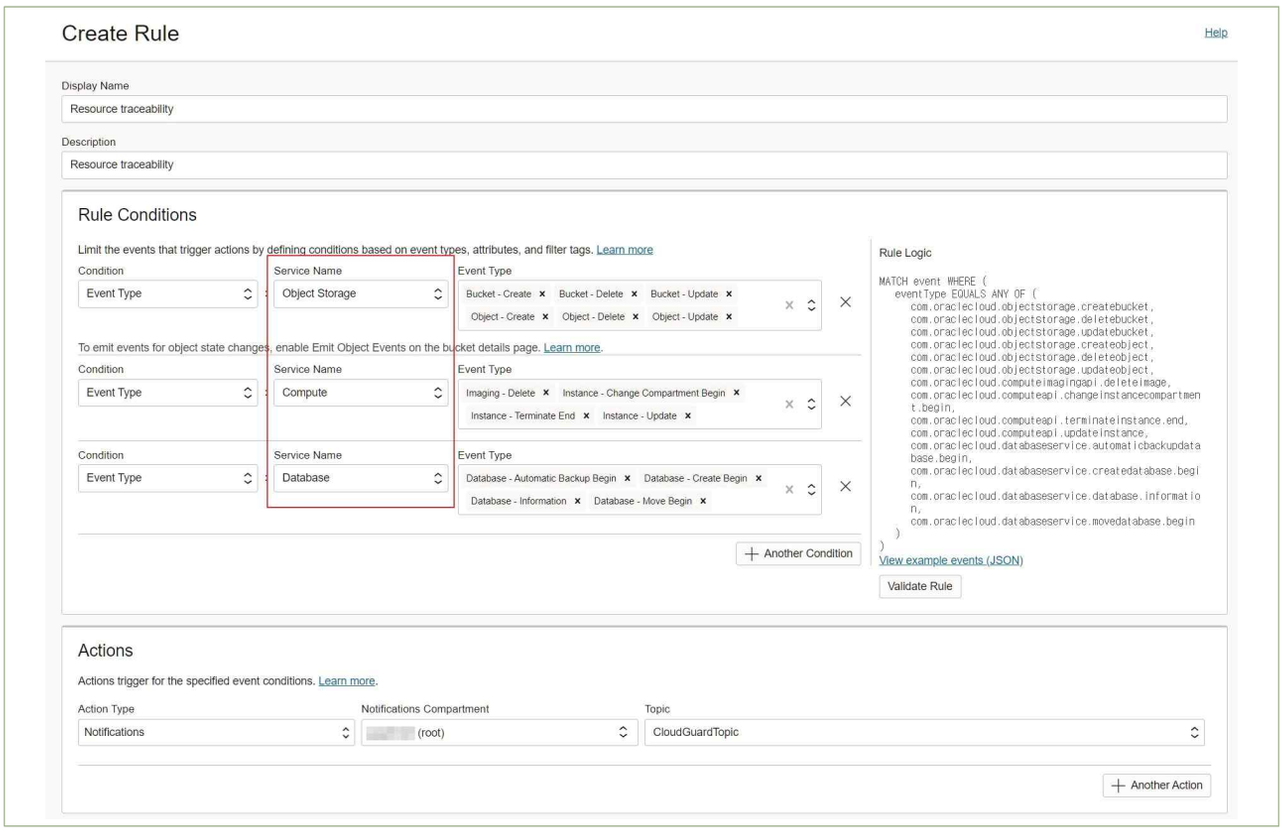
1) 가상 자원 변경 사항에 관한 행위(생성, 변경, 삭제 등)

- (OCI 콘솔) '홈' → 'Observability & Management' → 'Events Service' → 'Rules' → 'Create Rule'에서 가상 자원 리소스를 지정하여 행위 추적성 모니터링 기능



| 그림 5.1.1 | 가상 자원 이용 행위 추적성 모니터링 설정

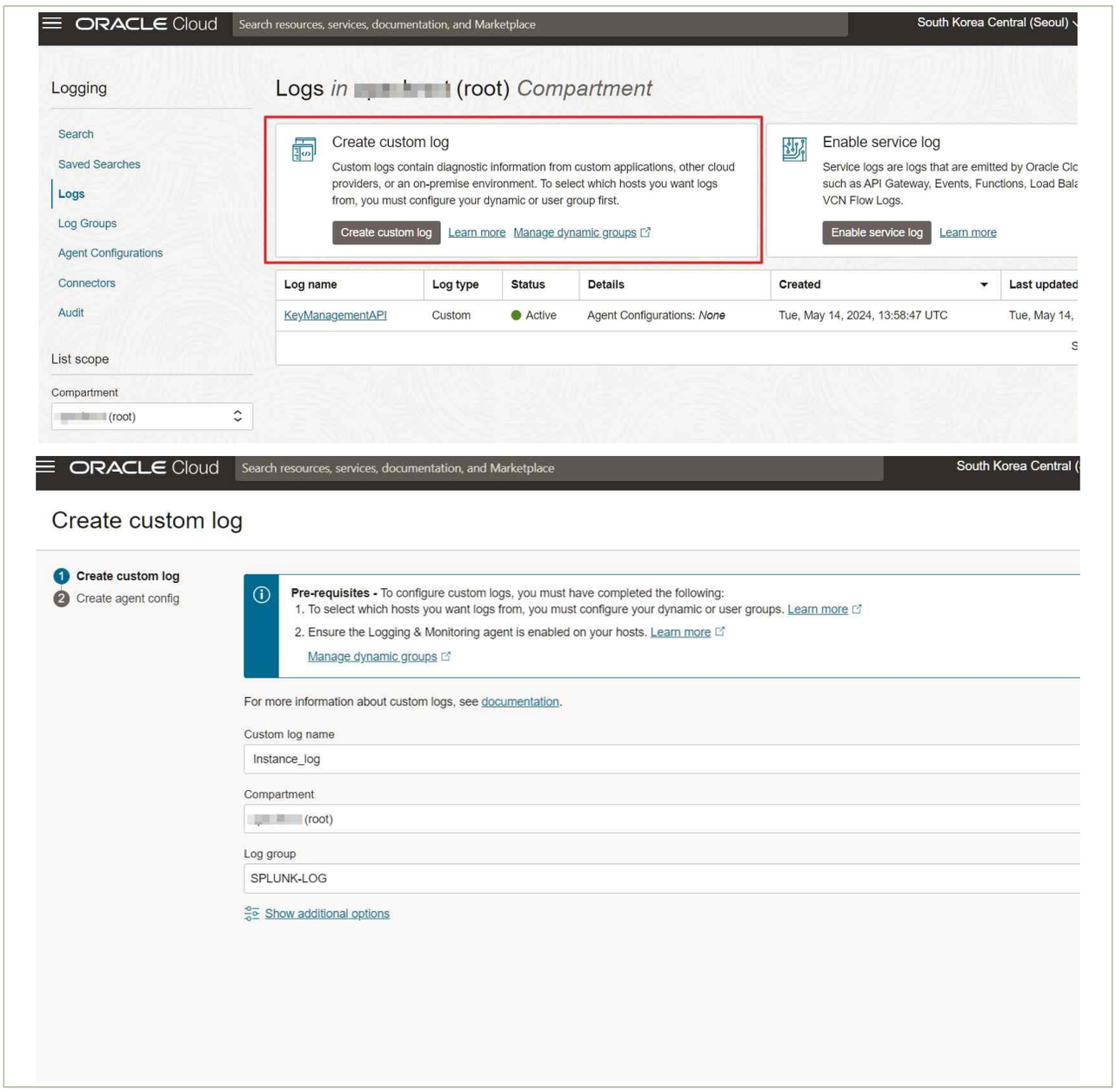
- 아래 메뉴 중 Actions → 'Notification' → 'Compartment' → 생성한 Topic을 지정하면 알림을 받고자 하는 메일 및 Slack 등으로 가상 자원의 행위를 지속적으로 알림을 받아볼 수 있음



| 그림 5.1.2 | 리소스 설정 및 관리자 알림 설정

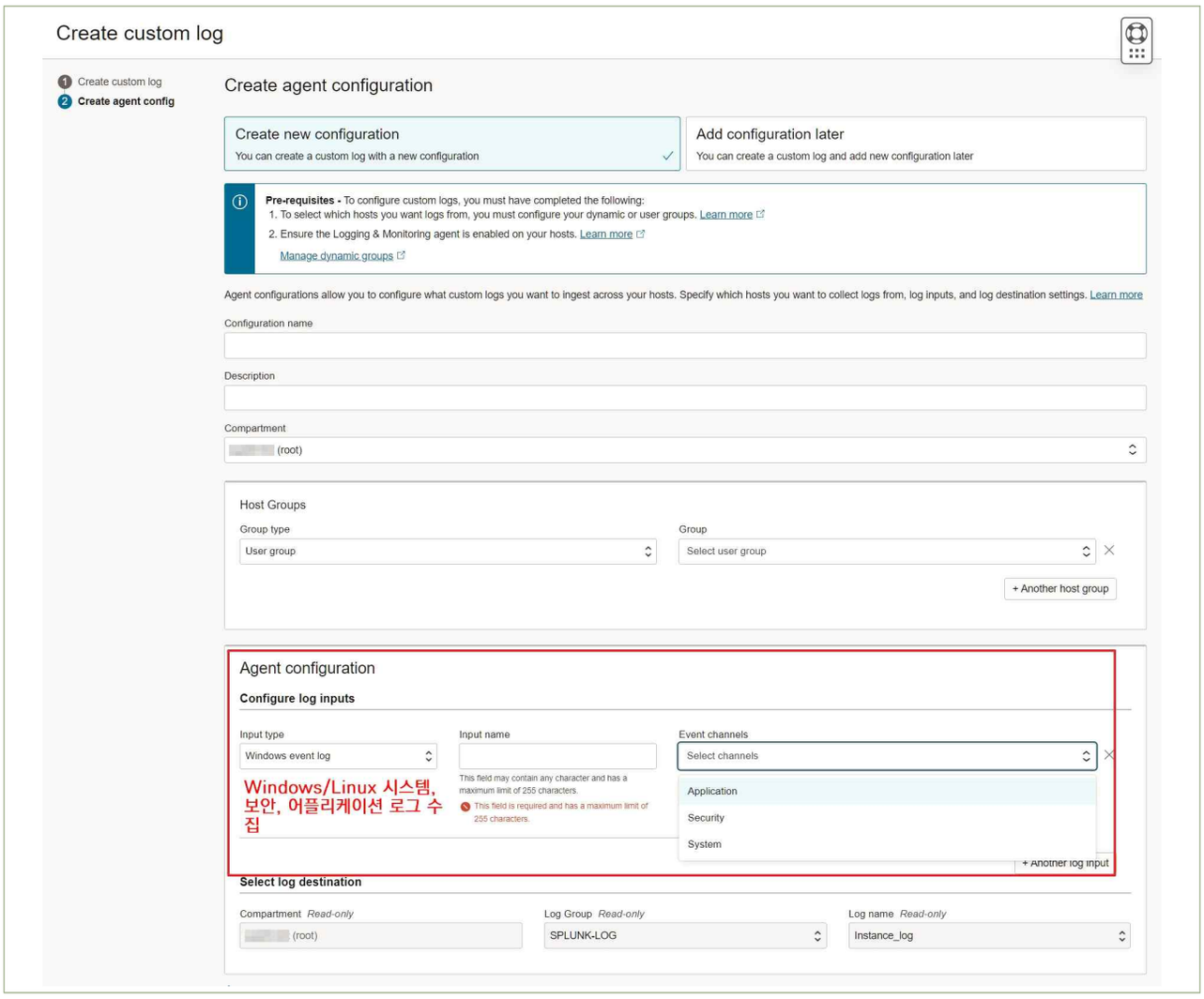
2) 가상 자원에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록

- (OCI 콘솔) '홈' → 'Observability & Management' → 'Logging' → 'Logs' → 'Create custom log'에서 가상 자원의 시스템 로그를 수집하여 접속 일시, 접속자 및 접근기록(Log) 확인 가능



| 그림 5.1.3 | 가상 자원의 Audit, Security, System log 수집

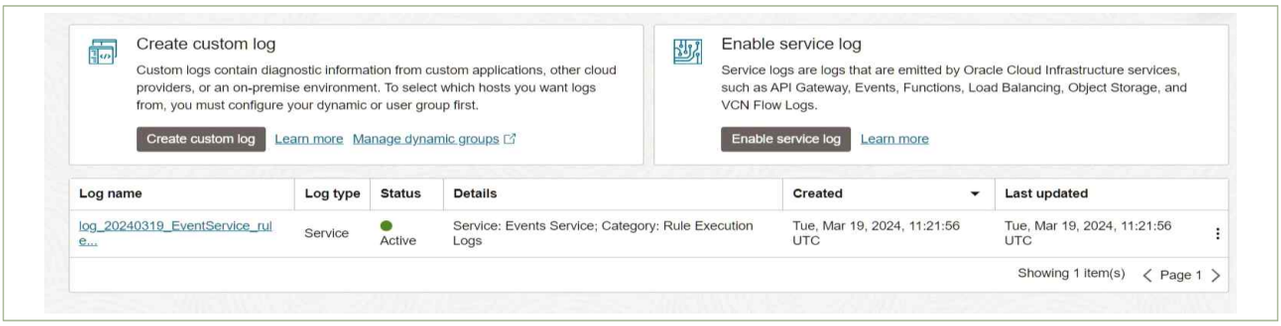
- Agent configuration을 통해 Input type: Windows, Linux(path)를 지정하여 다양한 시스템 로그를 수집하도록 지원



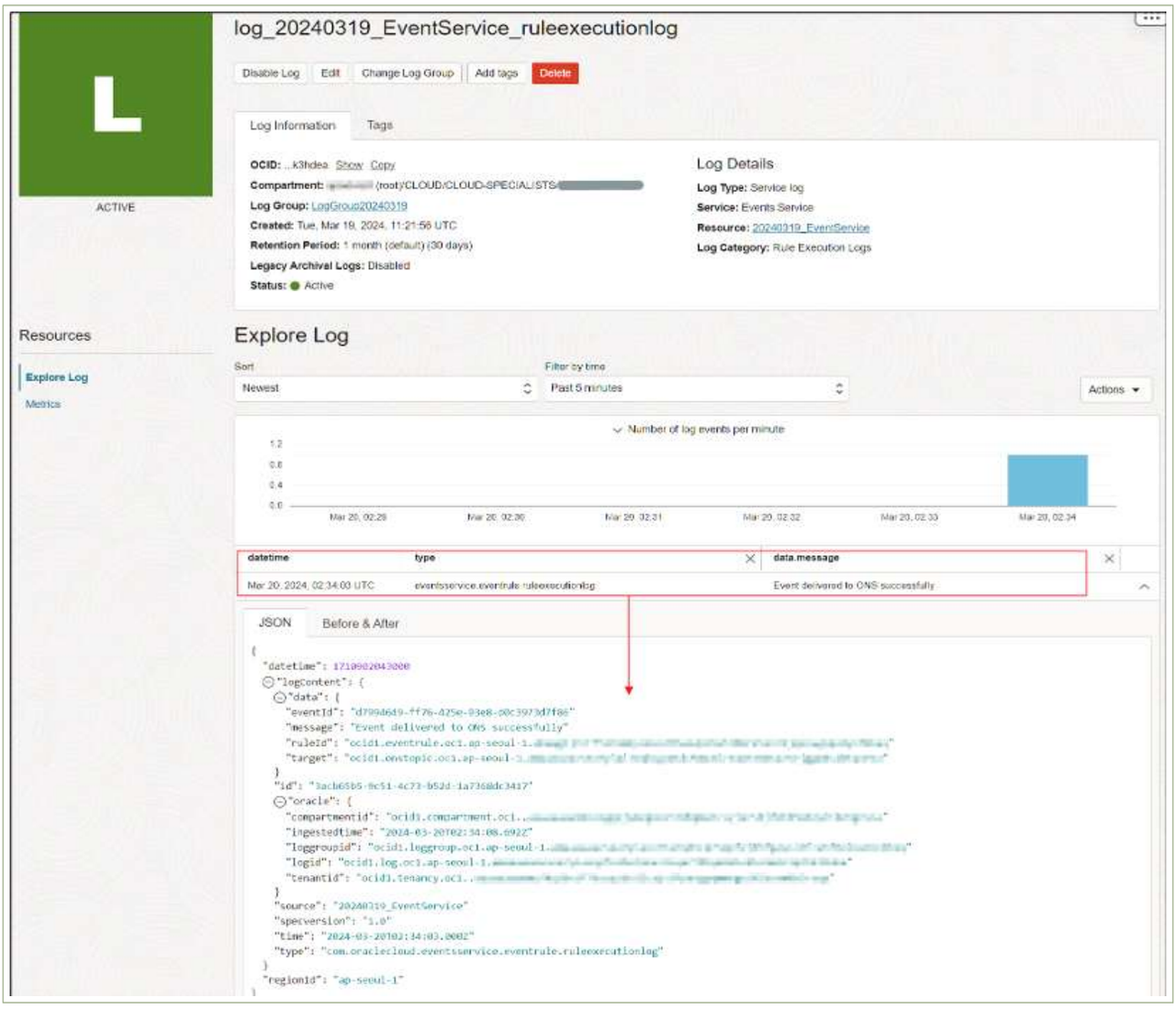
| 그림 5.1.4 | Agent Configuration 화면

3) 가상 자원을 이용한 일시, 사용자 및 가상 자원의 형태(서버, 데이터베이스, 스토리지 등) 확인할 수 있는 접근기록

- (OCI 콘솔) '홈' → 'Observability & Management' → 'Logging' → 'Logs' → '생성한 Log 선택'에서 계정 변경, 네트워크 변경 등 다양한 보안 모니터링에 대한 주기적인 검토가 가능하도록 지원

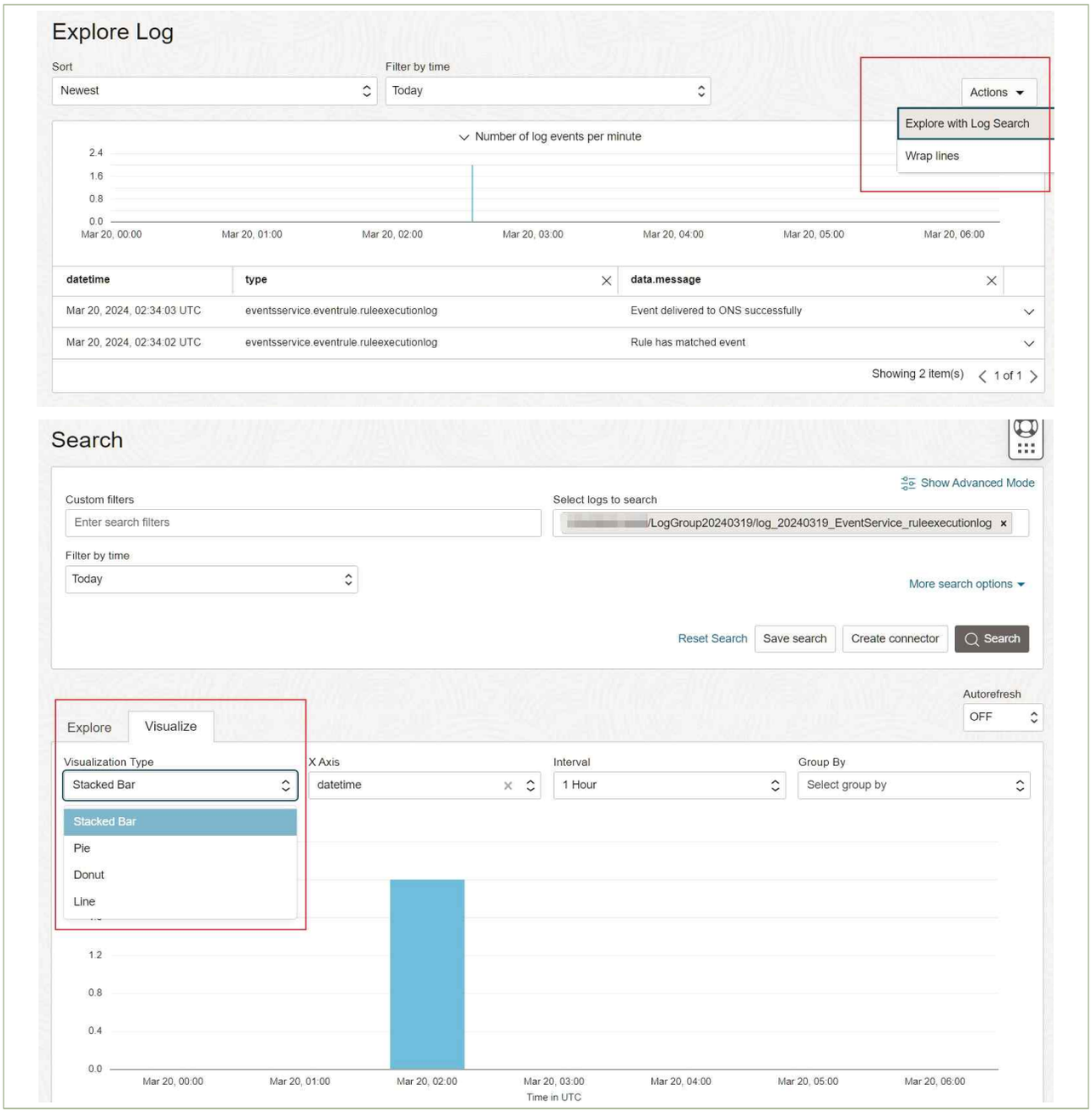


| 그림 5.1.5 | 접근기록을 저장하기 위한 Custom log 생성



| 그림 5.1.6 | 가상 자원 접근 기록 검토

- 검색된 로그에서 Actions → Explore with Log Search → Explorer or Visualize를 선택하여 원하는 필드나 로그 생성 시간 등을 조회할 수 있는 기능 제공



| 그림 5.1.7 | 로그 분석 기능 제공

4 참고 사항

- [Event Service] https://cloud.oracle.com/events/rules?region=ap-seoul-1
- [Logging] https://cloud.oracle.com/logging/logs?region=ap-seoul-1

1 기준

식별번호	기준	내용
5.2	**가상 자원 이용 행위 추적성 증적 모니터링**	가상 자원 이용에 관한 행위 추적성 증적에 대해 모니터링 및 주기적인 검토를 수행하여야 한다.

2 설명

- 클라우드 가상 자원 이용에 관한 행위 추적성 증적에 대해 모니터링 및 주기적인 검토를 수행하여야 한다.

  - 예시

    1) 클라우드 가상 자원 이용에 관한 행위 추적성 증적(ex. 감사 로그 등)에 대한 상시 모니터링 수행

    2) 금융회사 내부 규정 등 관련 규정을 통해 수립된 검토 기간에 맞추어 클라우드 가상 자원 이용에 관한 행위 추적성 증적에 대한 주기적인 검토 수행

3 우수 사례

- (주기적 검토) ‘5.1 가상 자원 이용에 관한 행위 추적성 확보’ 기준을 통해 확인된 로그에 대해 금융회사에서는 주기적으로 검토를 수행한다.

  - 인가받지 않은 가상 자원 접속, 생성, 변경, 삭제 등

4 참고 사항

- N/A

1 기준

식별번호	기준	내용
5.3	**이용자 가상 자원 모니터링 기능 확보**	이용자 가상 자원 운용에 관한 모니터링 기능을 확보하여야 한다.

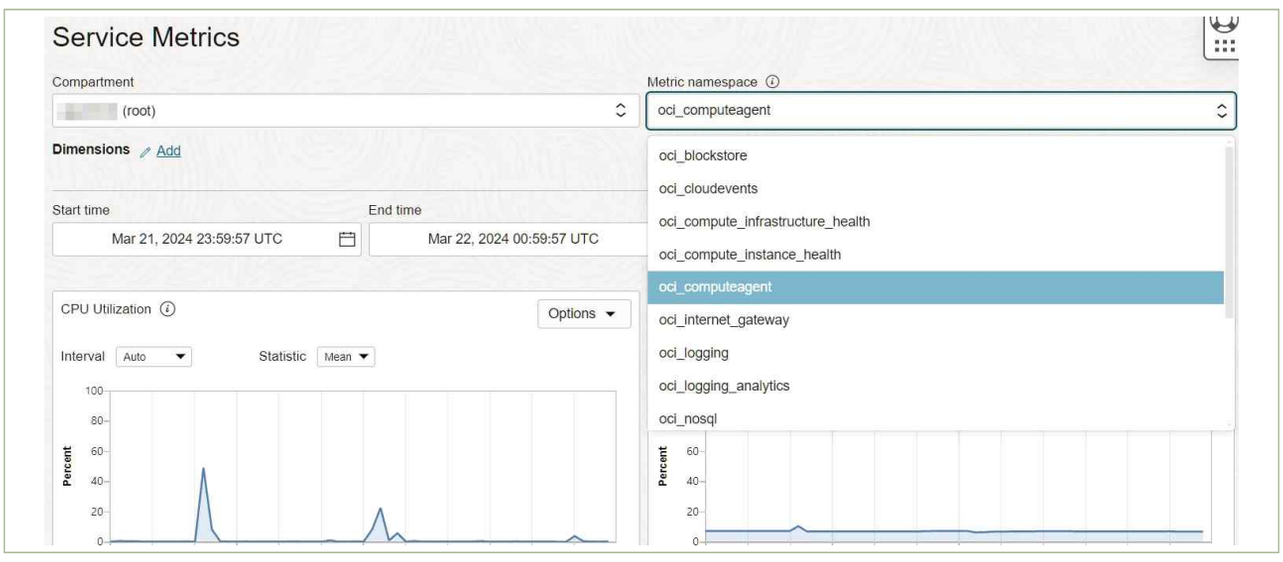
2 설명

- 이용자 가상 자원 가용성을 확보하고 장애대응을 위한 모니터링 기능을 확보하여야 한다.
  1) 가상 자원 상태 모니터링 (사용량, 트래픽 용량 등)
  2) 가상 자원 장애 모니터링 (장애 발생 시 담당자 공지 등)

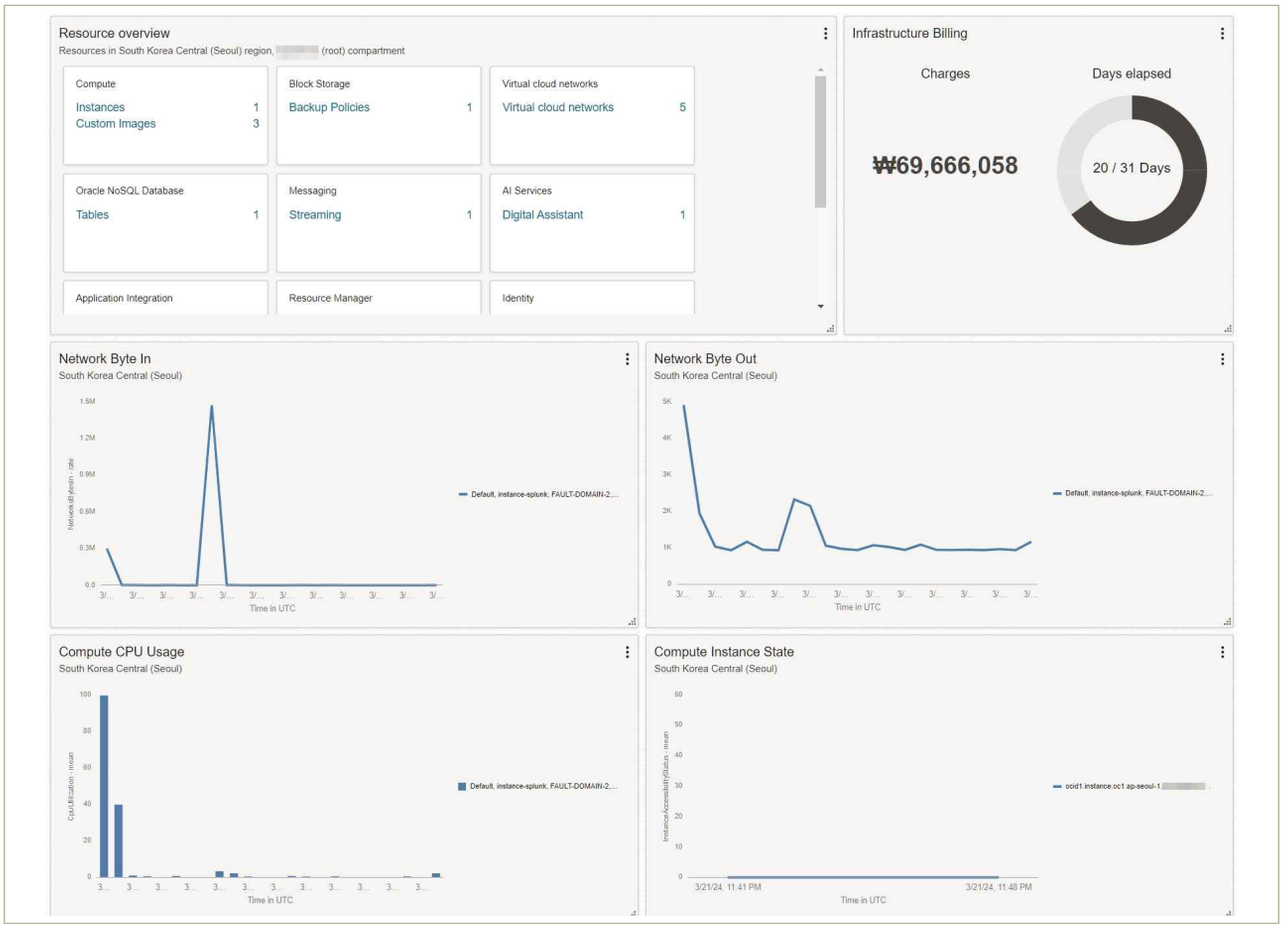
3 우수 사례

1) 가상 자원 상태 모니터링 (사용량, 트래픽 용량 등)

- (OCI 콘솔) '홈' → 'Observability & Management' → 'Monitoring' → 'Service Metrics'에서 서비스별 간략 모니터링 기능을 제공

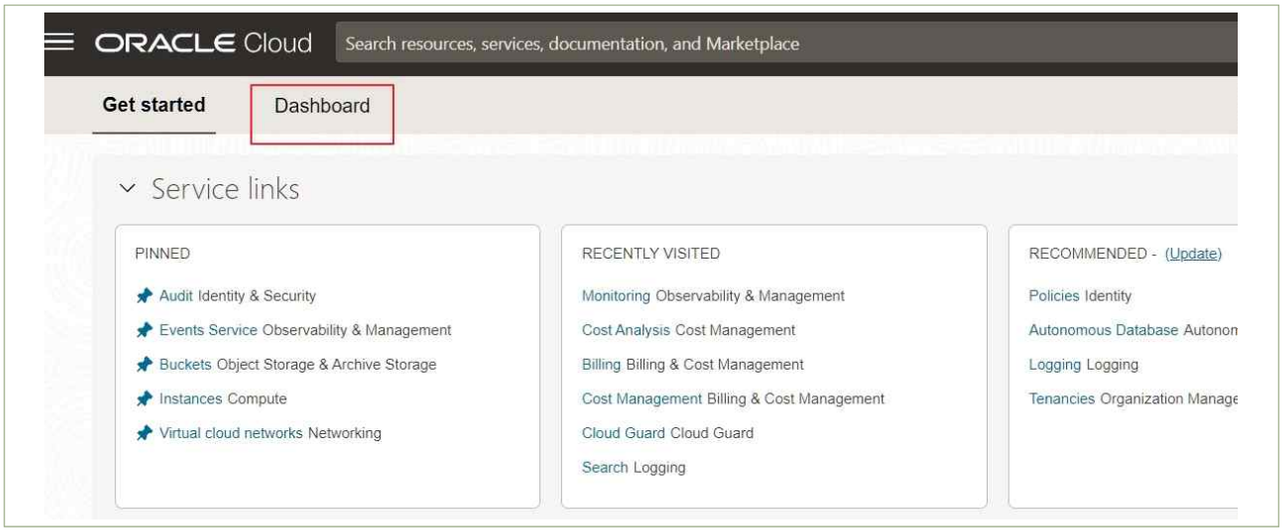


| 그림 5.3.1 | Metric 선택

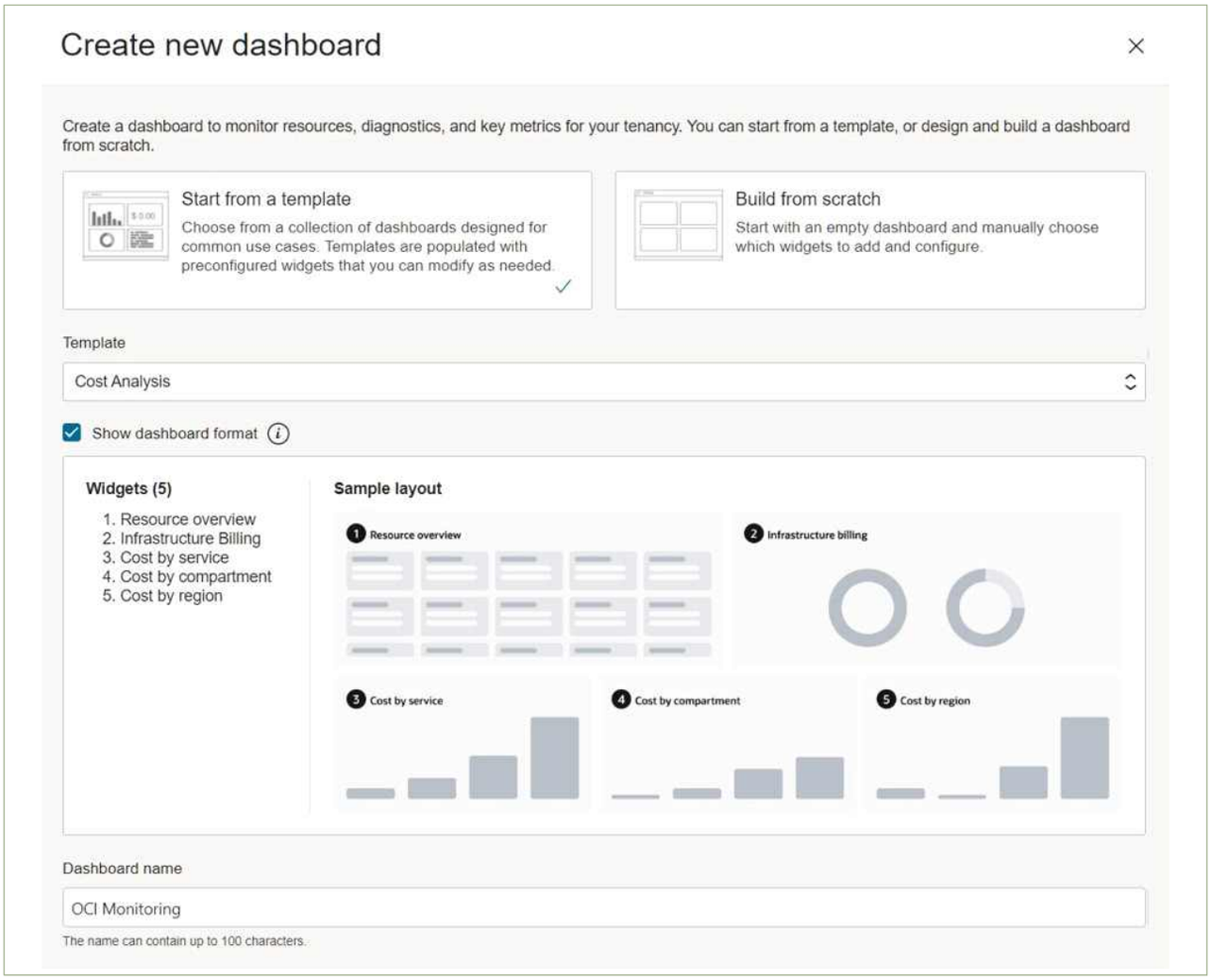


| 그림 5.3.2 | 모니터링 대시보드

- (OCI 콘솔) '홈' → '상단 Dashboard' 선택
  - 클라우드 리소스 등 필요한 모든 항목을 대시보드에 추가하여 모니터링이 가능

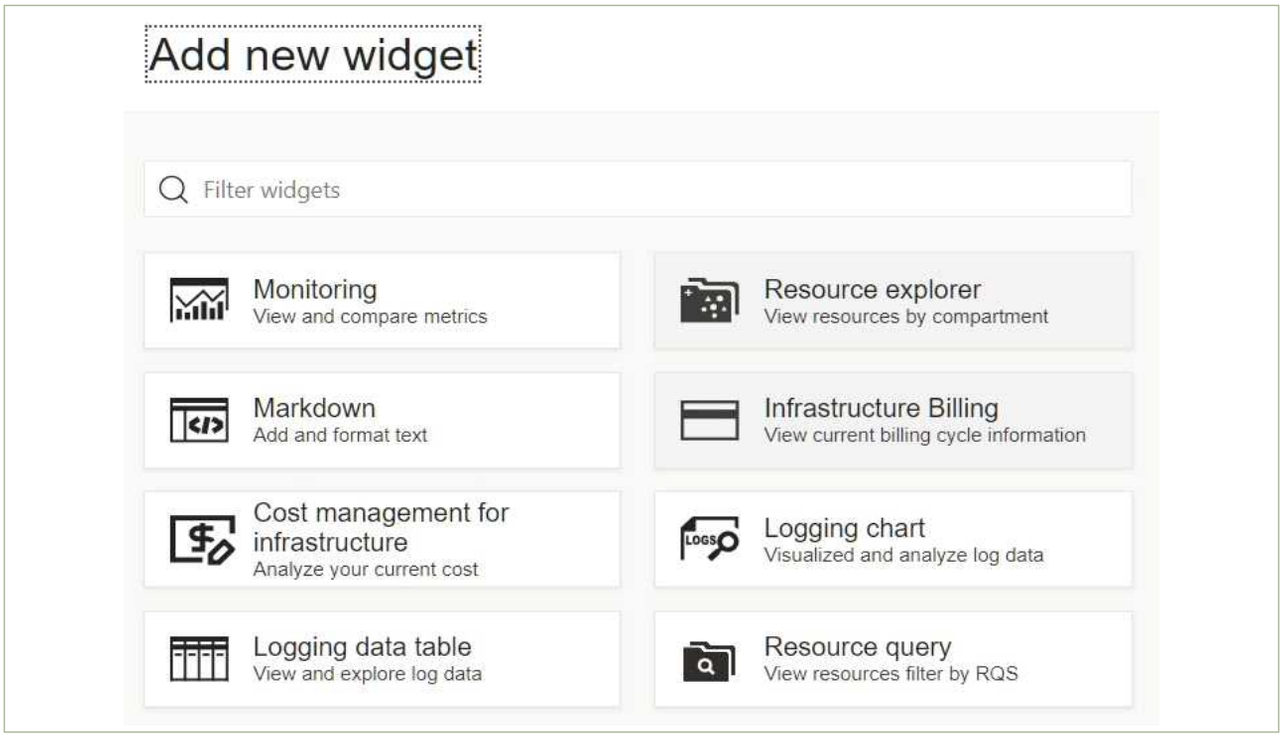


| 그림 5.3.3 | 대시보드 생성



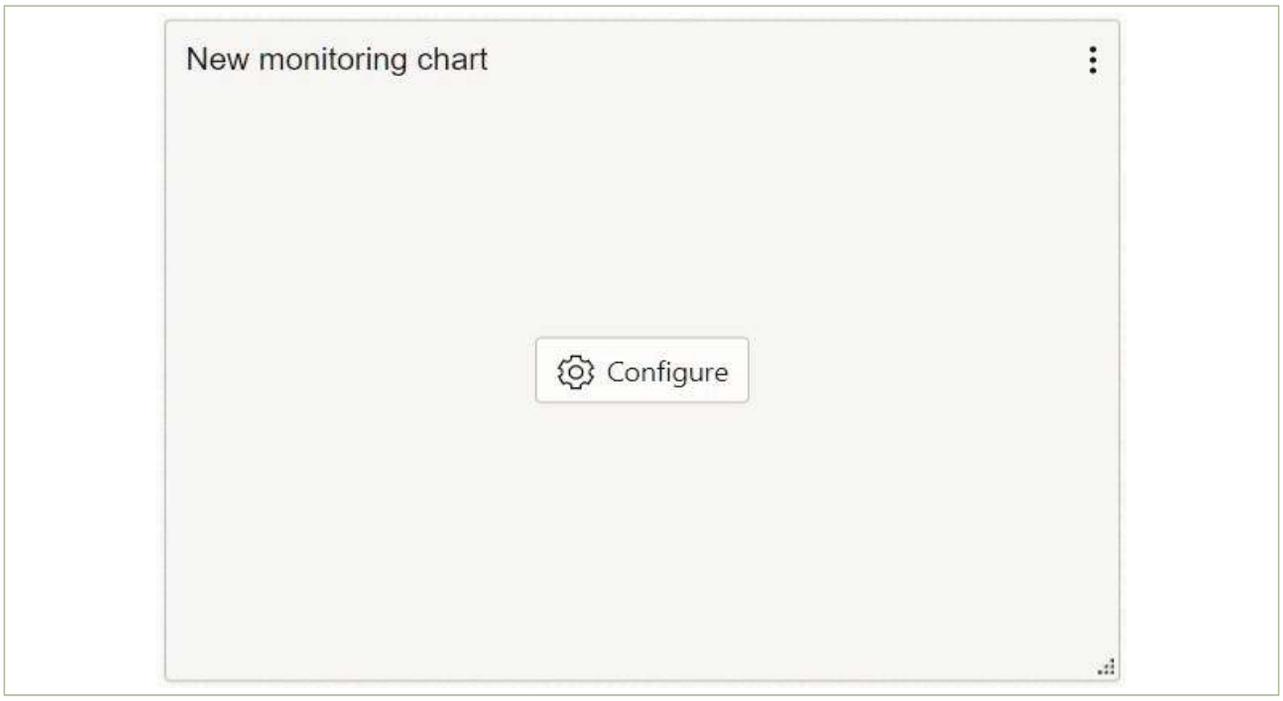
| 그림 5.3.4 | 대시보드 생성

- 대시보드 위젯 생성에서 Monitoring 및 Resource explorer 등을 선택하여 위젯을 생성할 수 있음

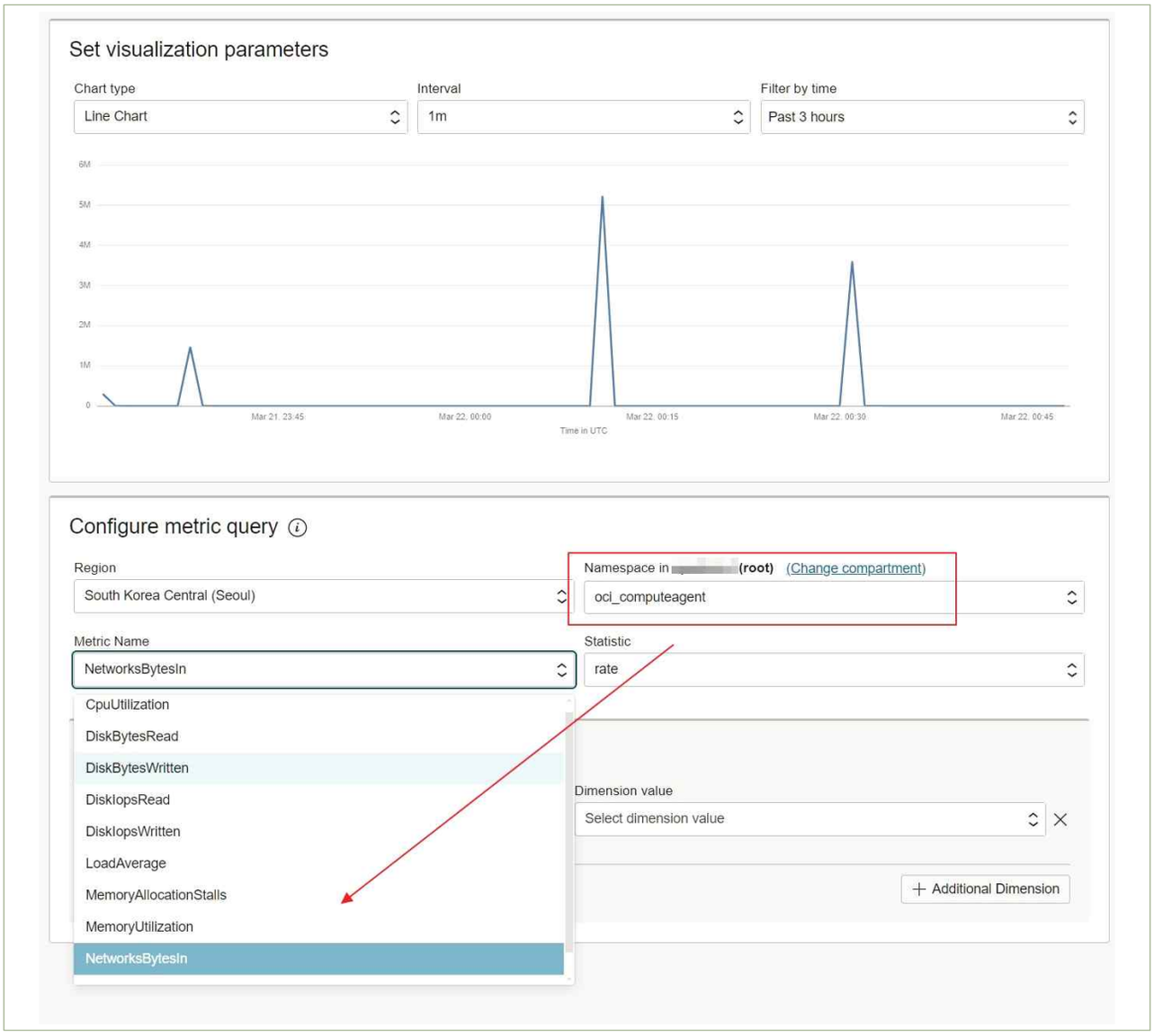


| 그림 5.3.5 | 위젯 생성

- 대시보드에 아래와 같은 레이아웃이 생성되며, Configure를 선택하여 모니터링 리소스 선택



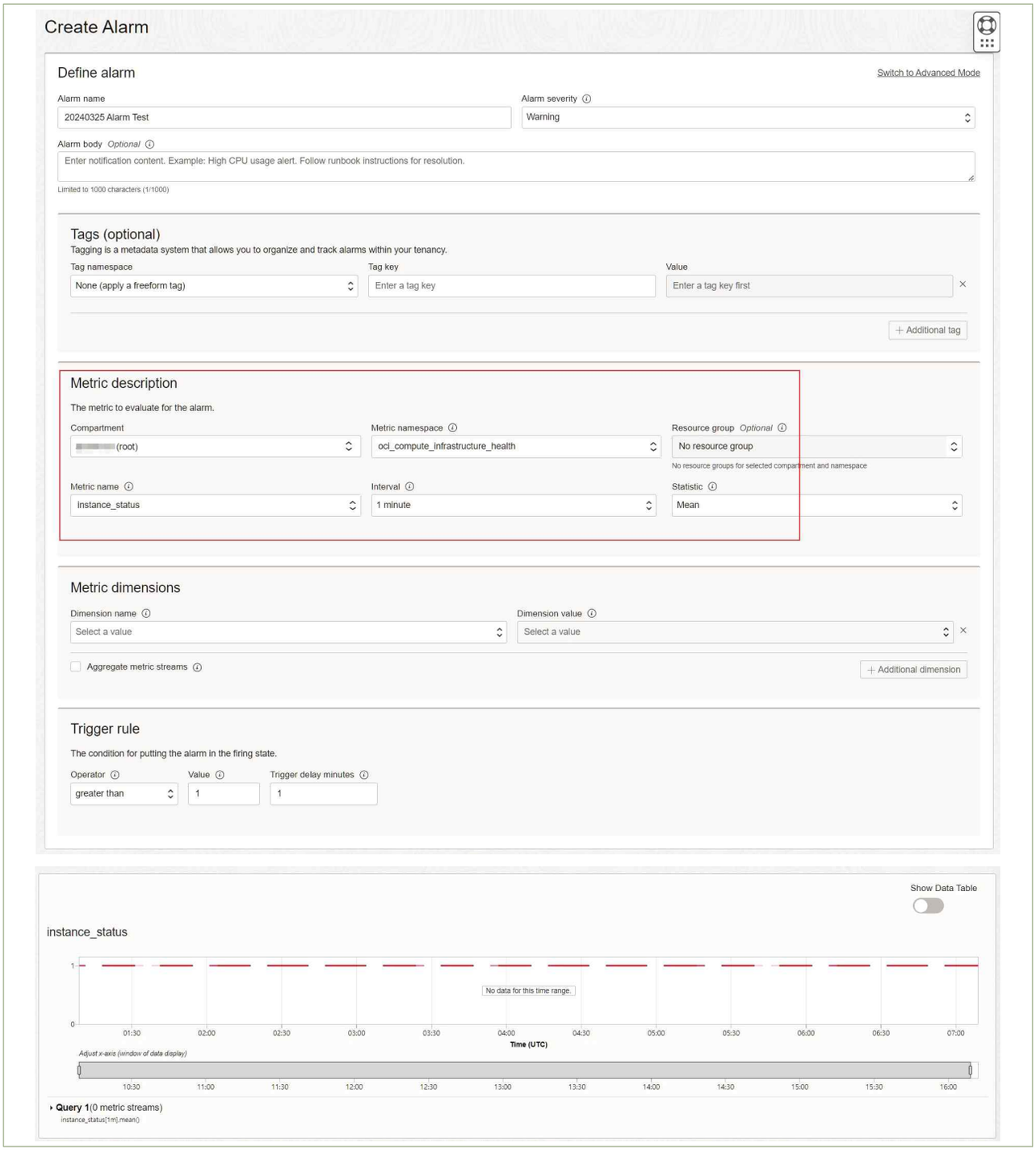
| 그림 5.3.6 | 레이아웃 생성 화면



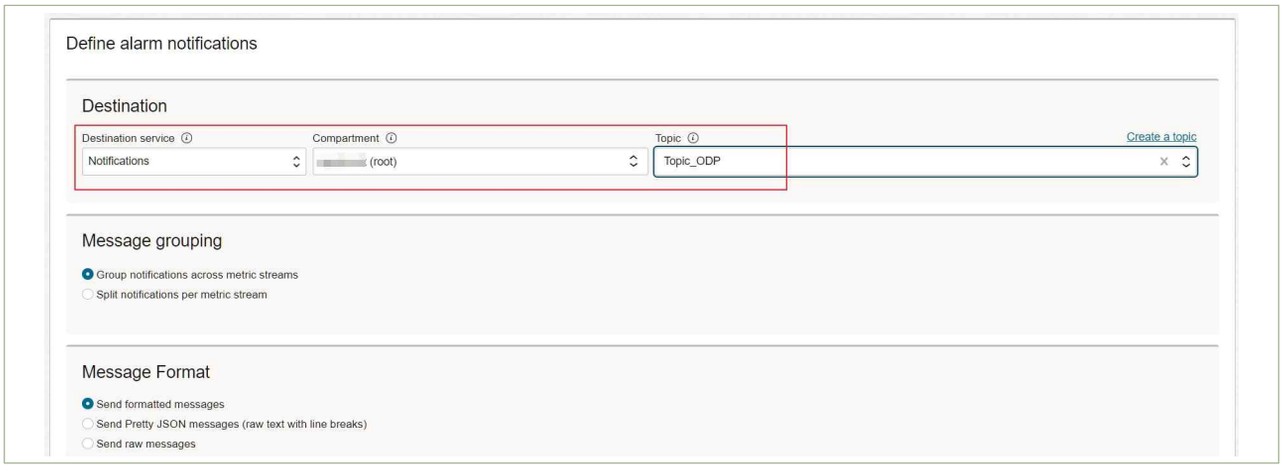
| 그림 5.3.7 | Configure metric query 화면

2) 가상 자원 장애 모니터링 (장애 발생 시 담당자 공지 등)

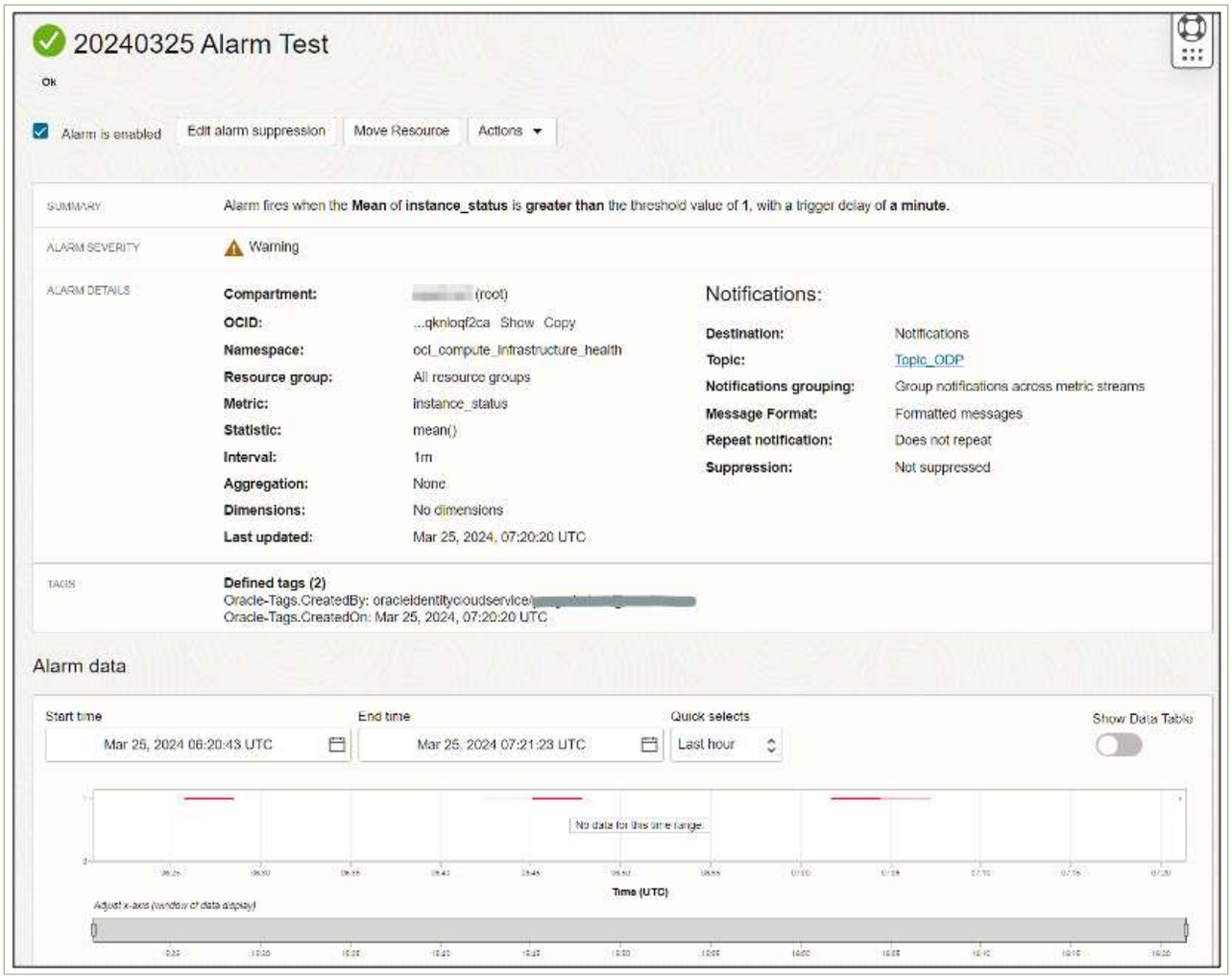
- (OCI 콘솔) '홈' → 'Observability & Management' → 'Monitoring' → 'Alarm Status'에서 장애 유형과 리소스 유형(Compute, Storage, Networking 등)을 지정하고, Notification Service의 Topic과 연동하여 담당자에게 관련 장애 유형별 알림을 받아볼 수 있도록 설정



| 그림 5.3.8 | 시스템에서 감지할 장애 유형 지정



| 그림 5.3.9 | 장애 발생 시 알람을 받을 담당자 지정

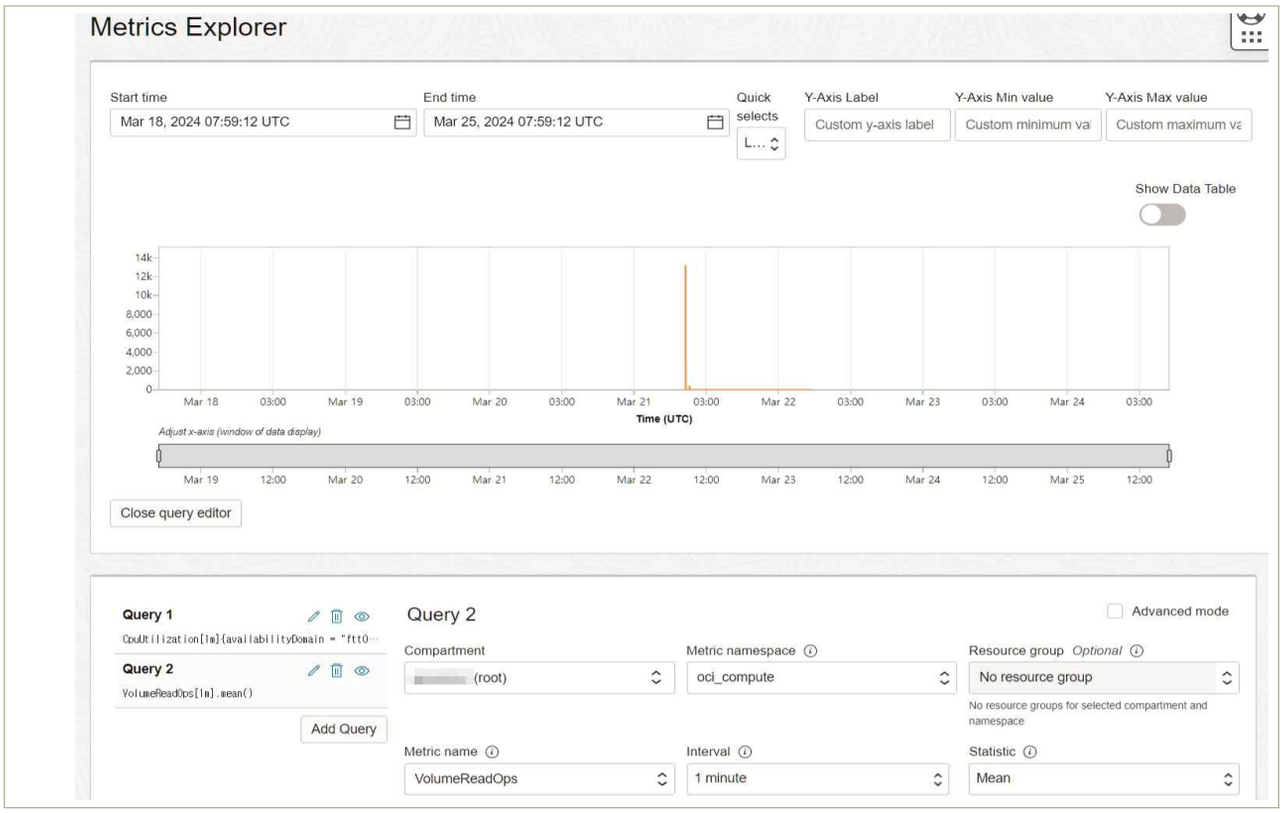


| 그림 5.3.10 | 장애발생 알림 설정 완료

- (OCI 콘솔) '홈' → 'Observability & Management' → 'Monitoring' → 'Health Checks'
  Health check 서비스를 통해 Instance(VM)를 지속적으로 모니터링

| 그림 5.3.11 | Health Check 설정 화면

- OCI 콘솔에서 Metrics Explorer 기능을 통해, 직접 모니터링 기능 제공



| 그림 5.3.12 | Metrics Explorer 화면

4 참고 사항

- [Monitoring] https://cloud.oracle.com/monitoring/?region=ap-seoul-1

1 기준

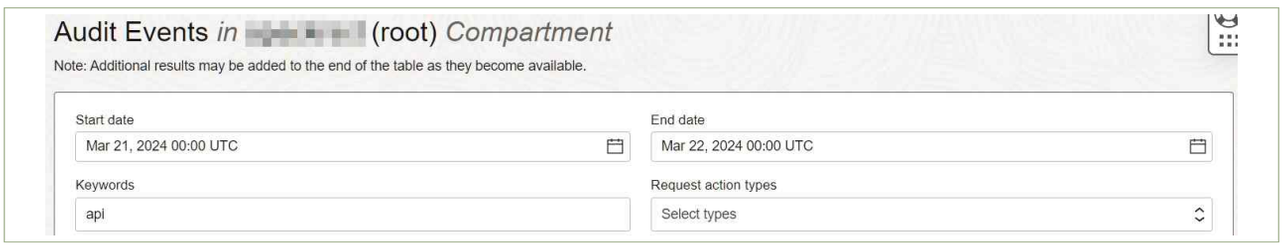
식별번호	기준	내용
5.4	**API 사용 (호출 대상, 호출자, 호출 일시 등)에 관한 행위 추적성 확보**	API 사용 이력에 대한 행위 추적성(로그 등)을 확보하여야 한다.

2 설명

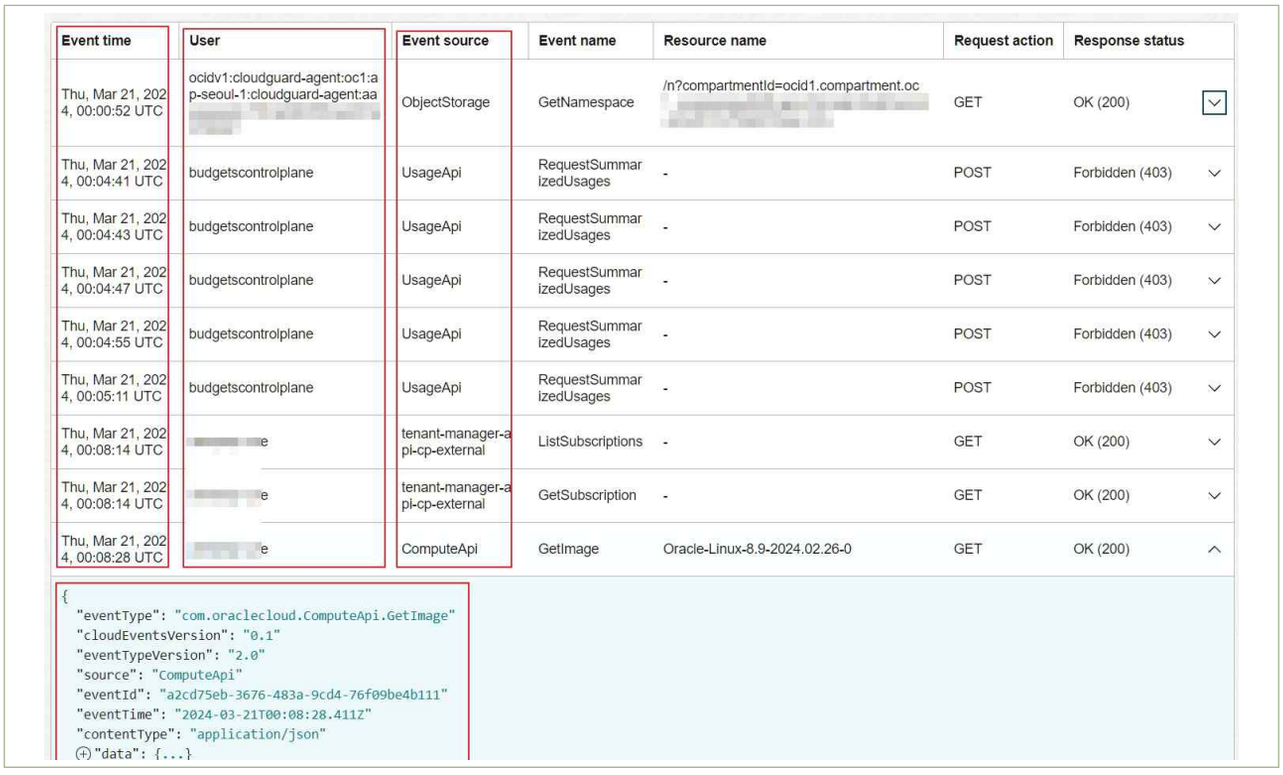
- API 사용 이력에 대한 행위 추적성을 확보하여야 한다.
  1) API 호출에 대한 정보(호출 대상, 호출자, 호출 일시 등)

3 우수 사례

- (가상 자원관리시스템) '홈' → 'Identity & Security' → 'Audit' → 'Keywords 검색'에서 'API' 키워드로 Audit Log 중 API 호출에 대한 정보 조회 기능을 제공(기간 등을 설정하여 세부 내용 조회)



| 그림 5.4.1 | 모니터링 대상 지정(API 사용)



Event time	User	Event source	Event name	Resource name	Request action	Response status
Thu, Mar 21, 2024, 00:00:52 UTC	ocidv1:cloudguard-agent:oc1:ap-seoul-1:cloudguard-agent:aa	ObjectStorage	GetNamespace	/n?compartmentId=ocid1.compartment.oc	GET	OK (200)
Thu, Mar 21, 2024, 00:04:41 UTC	budgetscontrolplane	UsageApi	RequestSummarizedUsages	-	POST	Forbidden (403)
Thu, Mar 21, 2024, 00:04:43 UTC	budgetscontrolplane	UsageApi	RequestSummarizedUsages	-	POST	Forbidden (403)
Thu, Mar 21, 2024, 00:04:47 UTC	budgetscontrolplane	UsageApi	RequestSummarizedUsages	-	POST	Forbidden (403)
Thu, Mar 21, 2024, 00:04:55 UTC	budgetscontrolplane	UsageApi	RequestSummarizedUsages	-	POST	Forbidden (403)
Thu, Mar 21, 2024, 00:05:11 UTC	budgetscontrolplane	UsageApi	RequestSummarizedUsages	-	POST	Forbidden (403)
Thu, Mar 21, 2024, 00:08:14 UTC	e	tenant-manager-api-cp-external	ListSubscriptions	-	GET	OK (200)
Thu, Mar 21, 2024, 00:08:14 UTC	e	tenant-manager-api-cp-external	GetSubscription	-	GET	OK (200)
Thu, Mar 21, 2024, 00:08:28 UTC	e	ComputeApi	GetImage	Oracle-Linux-8.9-2024.02.26-0	GET	OK (200)


```
{
  "eventType": "com.oraclecloud.ComputeApi.GetImage"
  "cloudEventsVersion": "0.1"
  "eventTypeVersion": "2.0"
  "source": "ComputeApi"
  "eventId": "a2cd75eb-3676-483a-9cd4-76f09be4b111"
  "eventTime": "2024-03-21T00:08:28.411Z"
  "contentType": "application/json"
  ⊕"data": {...}
```


| 그림 5.4.2 | 모니터링 대상 지정(API 사용)

4 참고 사항

- https://cloud.oracle.com/audit/events?region=ap-seoul-1

1 기준

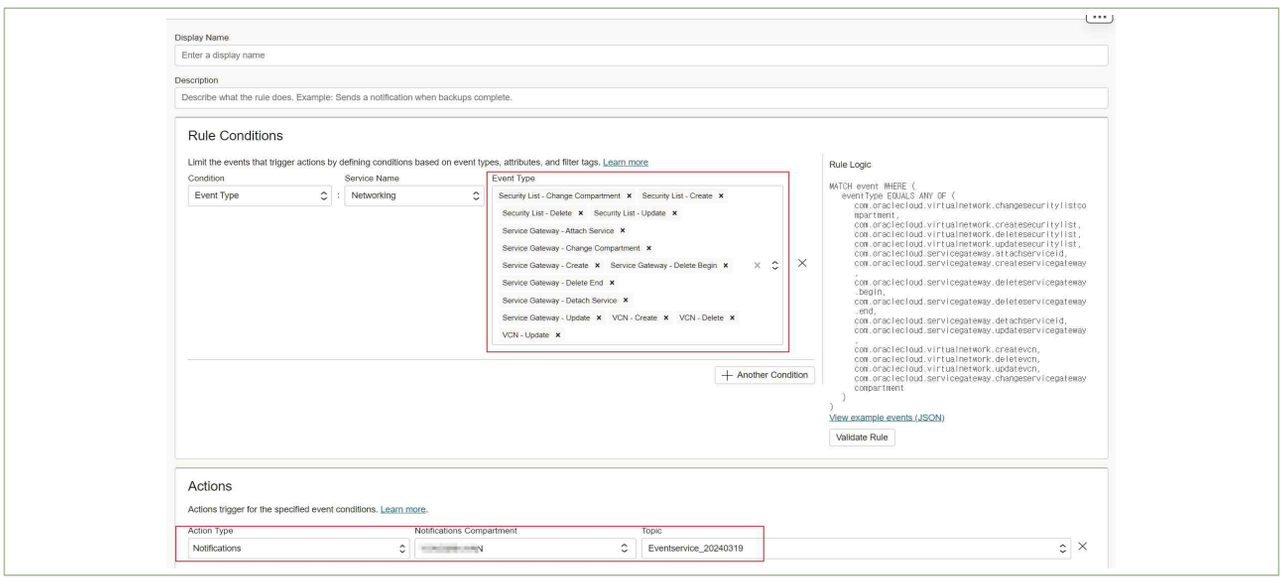
식별번호	기준	내용
5.5	**네트워크 관련 서비스(VPC, 보안 그룹, ACL 등)에 관한 행위 추적성 확보**	이용자의 클라우드 네트워크 서비스 이용 시 발생하는 사항에 대한 행위 추적성(로그 등)을 확보하여야 한다.

2 설명

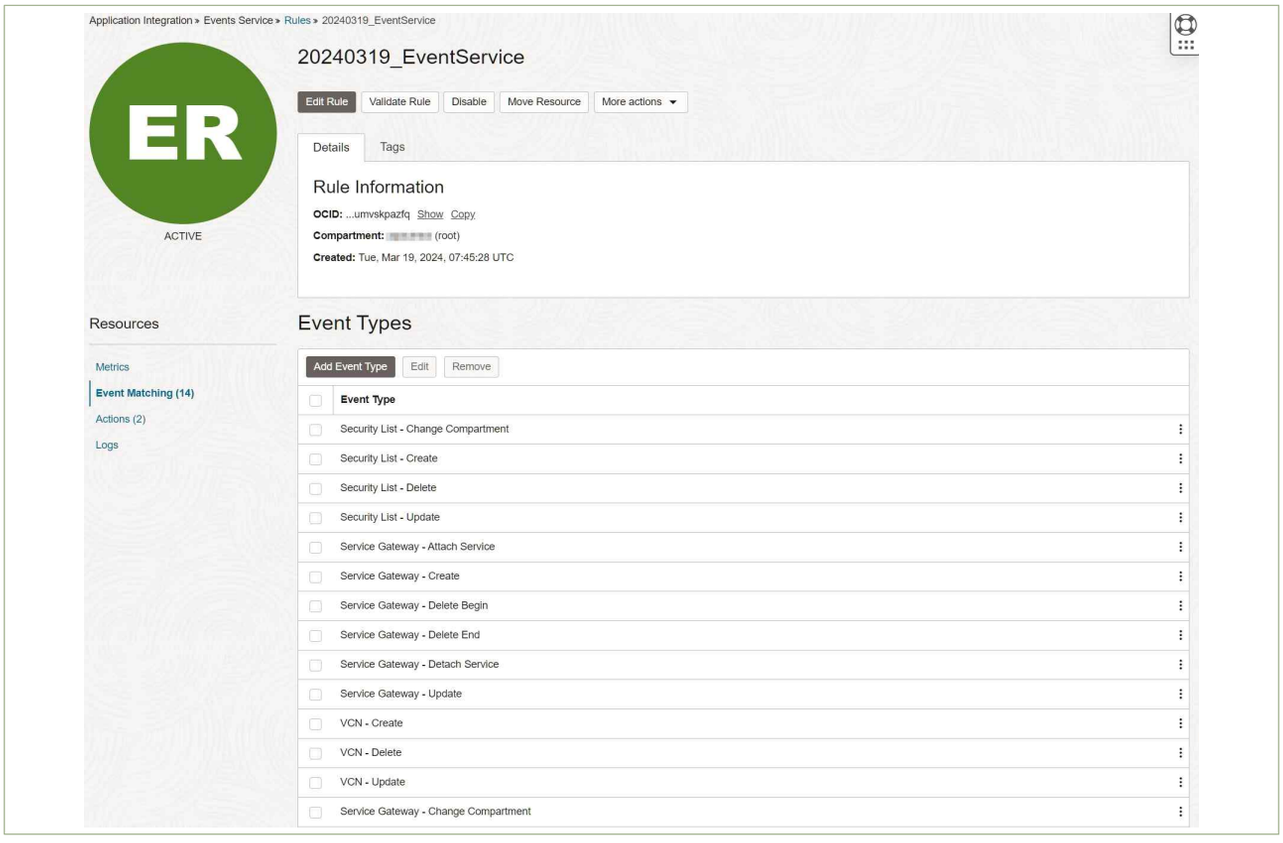
- 클라우드 환경에서 네트워크 서비스(VPC, NAT 등) 사용 시 발생하는 사항에 대한 행위 추적성(로그 등)을 확보하여야 한다.
  1) 네트워크 서비스 이용에 관한 사항(VPC, NAT 규칙 생성 및 변경 등) 등

3 우수 사례

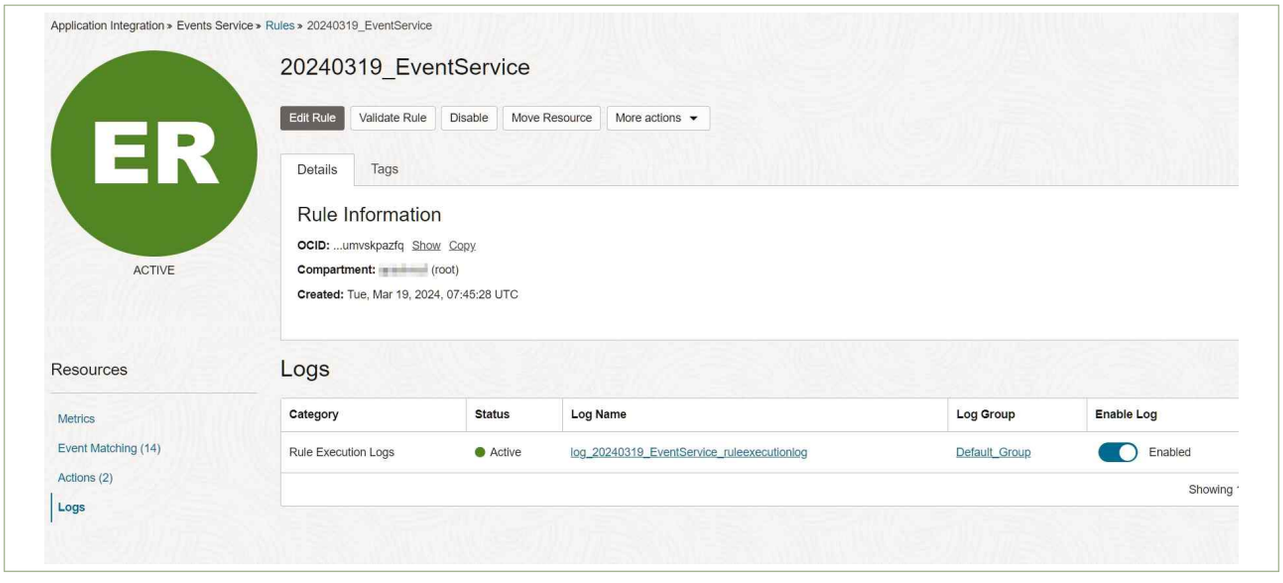
- (OCI 콘솔) '홈' → 'Observability & Management' → 'Events Service' → 'Create Rule'에서 Rule conditions → 'Condition' → 'Service Name' → 'Networking' → 'Event type' → VCN, Security List, NAT 등 네트워크 서비스 사용 시 발생하는 사항에 대해 모니터링(Notification Email, SMS 등) 기능을 제공



| 그림 5.5.1 | 모니터링 대상 지정(Networking)

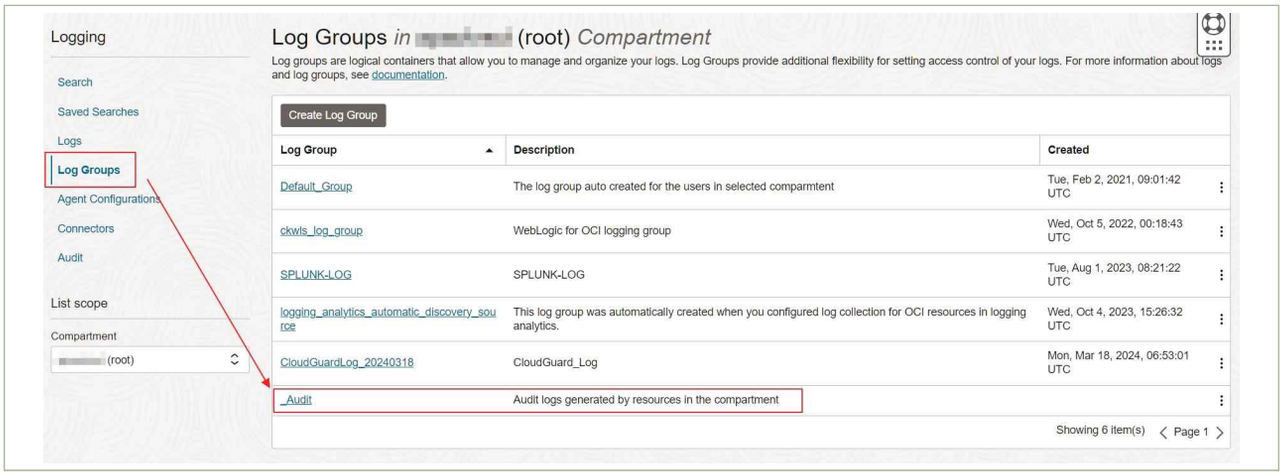


| 그림 5.5.2 | 네트워크 행위 추적성 설정 상태 확인

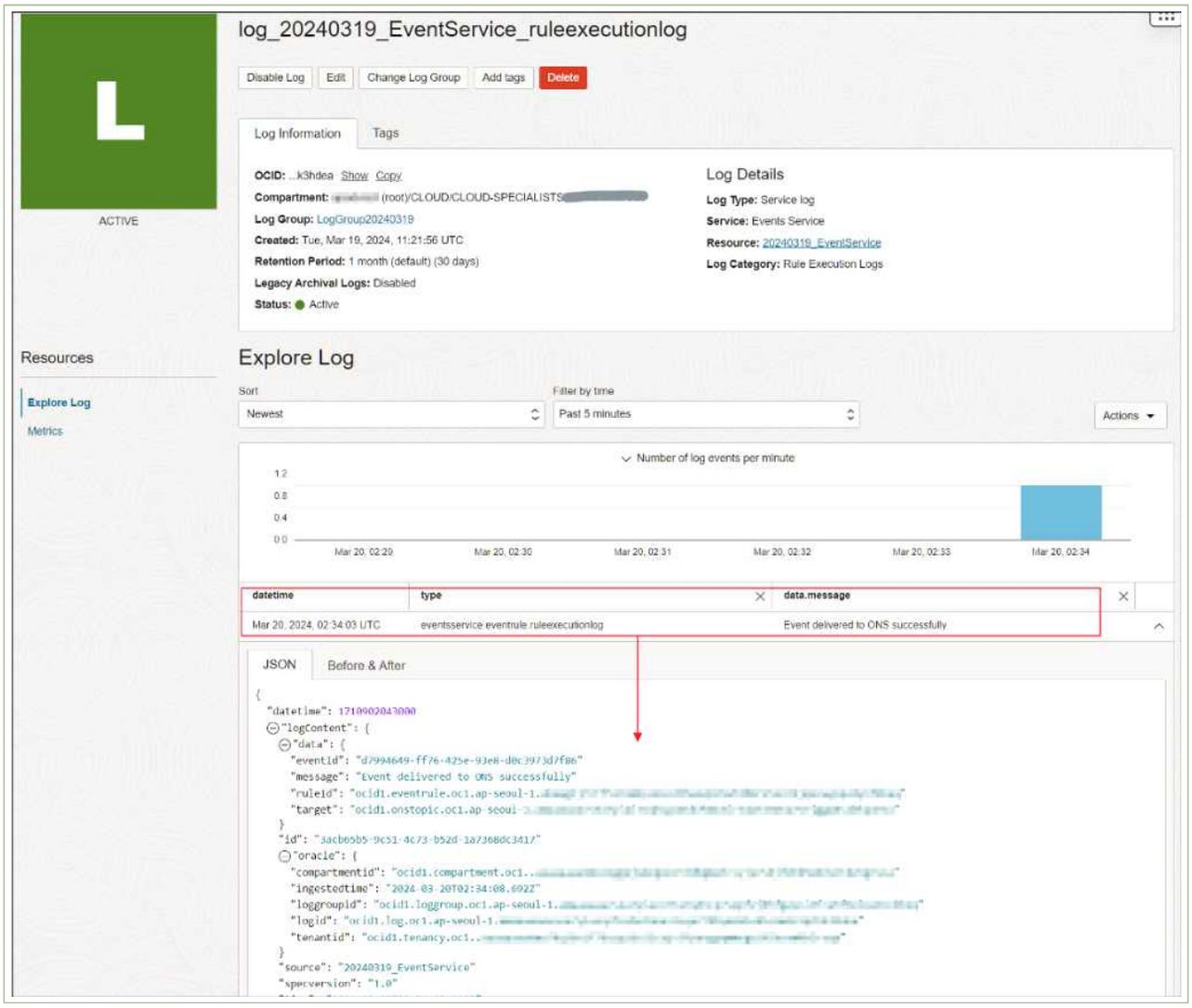


| 그림 5.5.3 | 행위 추적성 로깅 활성화

- 리소스 변경 사항의 행위추적성은 Logs로 남겨 추후 지속적으로 검토할 수 있도록 제공
- Logs → Enable Log → 활성화 (로그 저장을 위해 Log Group 생성 필요)



| 그림 5.5.4 | Log Group 생성



| 그림 5.5.5 | 네트워크 리소스 행위 추적성 확인

4 참고 사항

- [Event Service] https://cloud.oracle.com/events/rules?region=ap-seoul-1
- [Logging] https://cloud.oracle.com/logging/logs?region=ap-seoul-1

1 기준

식별번호	기준	내용
5.6	**계정 변동 사항에 대한 행위 추적성 확보**	클라우드 계정 변동 사항에 대한 행위 추적성(로그 등)을 확보하여야 한다.

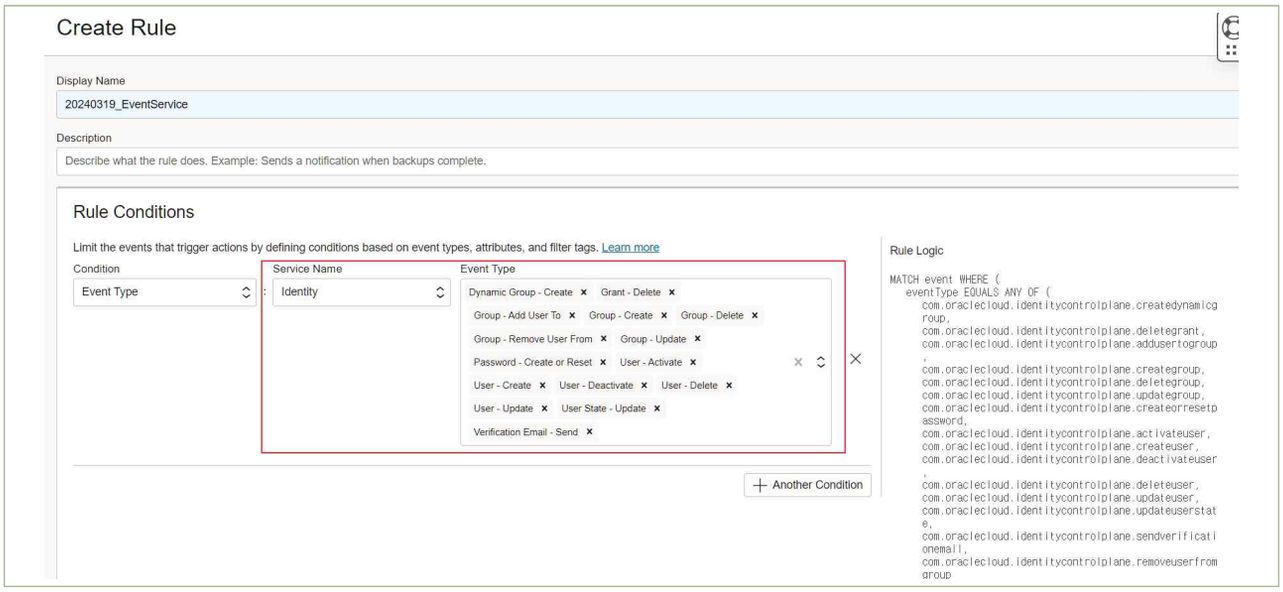
2 설명

- 클라우드 계정 변동 사항에 대한 행위 추적성(로그 등)을 확보하여야 한다.
  1) 클라우드 OCI 콘솔 접속 계정 생성, 변경, 삭제에 관한 사항
  2) 클라우드 가상 자원(서버, 데이터베이스 등) 접속 계정 생성, 변경, 삭제에 관한 사항

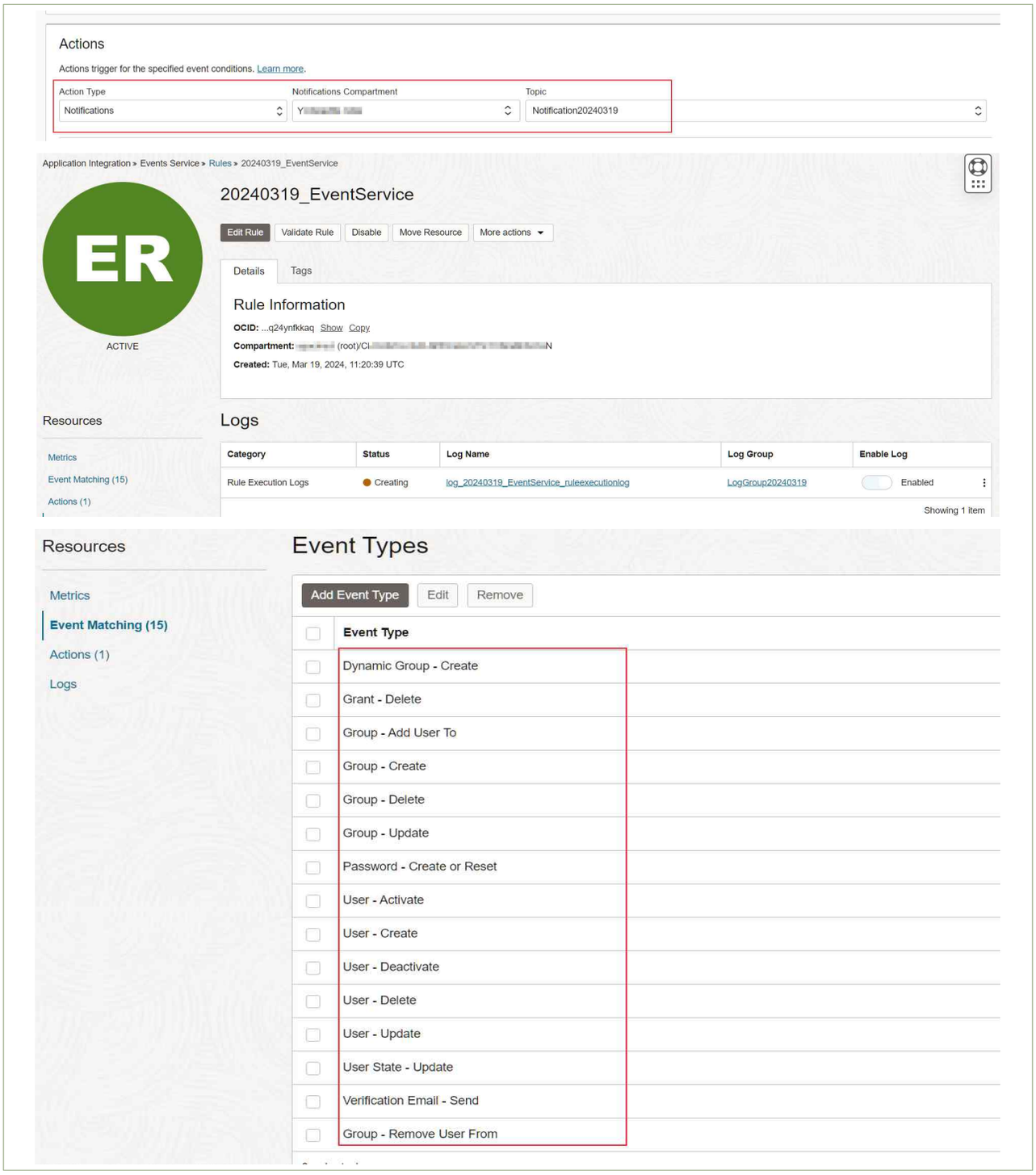
3 우수 사례

1) 클라우드 가상 자원 관리시스템 접속 계정 생성, 변경, 삭제에 관한 사항

- (가상 자원관리시스템) '홈' → 'Observability & Management' → 'Events Service' → 'Create Rule'에서 Rule conditions → 'Condition' → 'Service Name' → 'Identity' → 'Event type' → 계정 변경 사항(생성, 삭제 등)에 대해 모니터링(Notification Email, SMS 등) 및 로깅 기능을 제공



| 그림 5.6.1 | 모니터링 리소스 지정(Service Name을 Identity로 설정)



| 그림 5.6.2 | 모니터링 리소스 지정(계정정보 관련 이벤트를 모니터링) 및 알람설정

4 참고 사항

- [Event Service] https://cloud.oracle.com/events/rules?region=ap-seoul-1
- [Logging] https://cloud.oracle.com/logging/logs?region=ap-seoul-1

1 기준

식별번호	기준	내용
5.7	**계정 변경 사항에 관한 모니터링 수행**	클라우드 서비스 이용 계정 변경 사항(생성, 삭제 등)에 관한 로깅 및 모니터링을 수행하여야 한다.

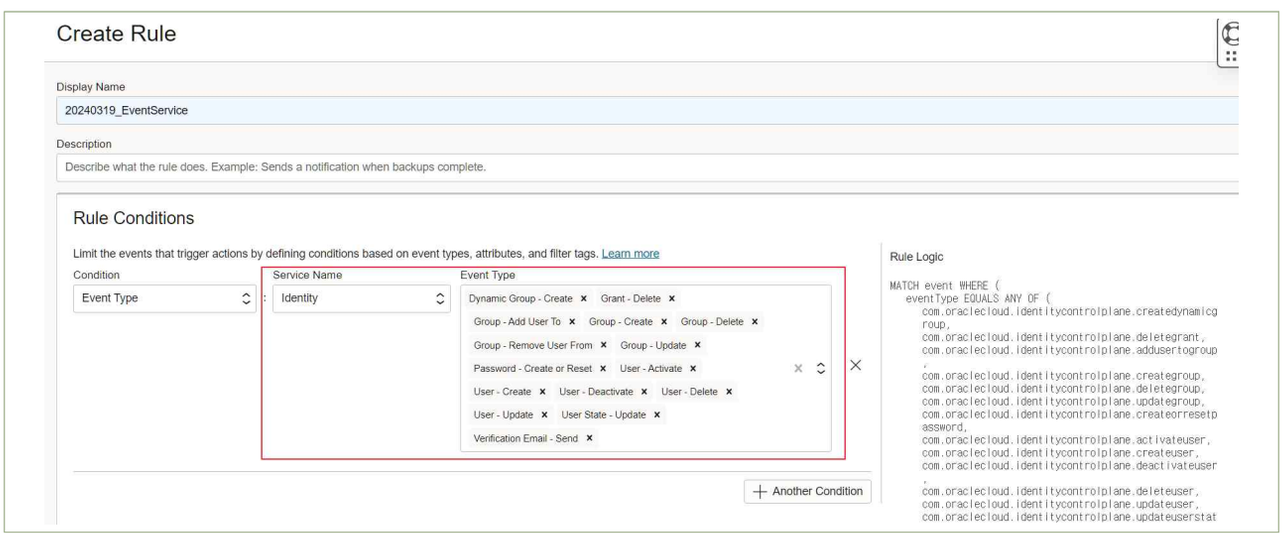
2 설명

- 클라우드 서비스 이용 계정 변경 사항에 관한 모니터링을 수행하여야 한다.
  1) 계정 변경 사항에 관한 상시 모니터링 수행
  2) 전자금융감독규정 및 금융회사 내부규정 등에 수립된 주기에 맞추어 주기적 검토 수행
  3) 관리자 계정에 대해서는 이중 확인 수행 등

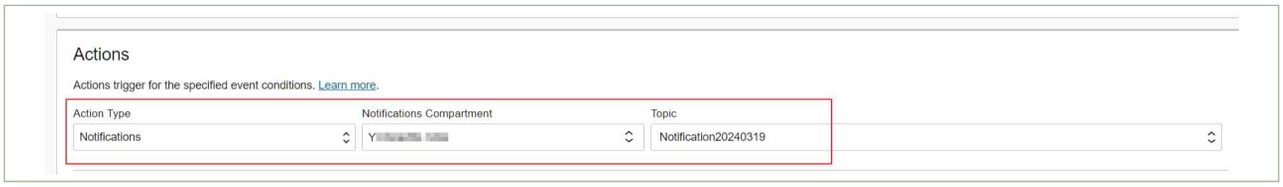
3 우수 사례

1) 계정 변경 사항에 관한 상시 모니터링 수행

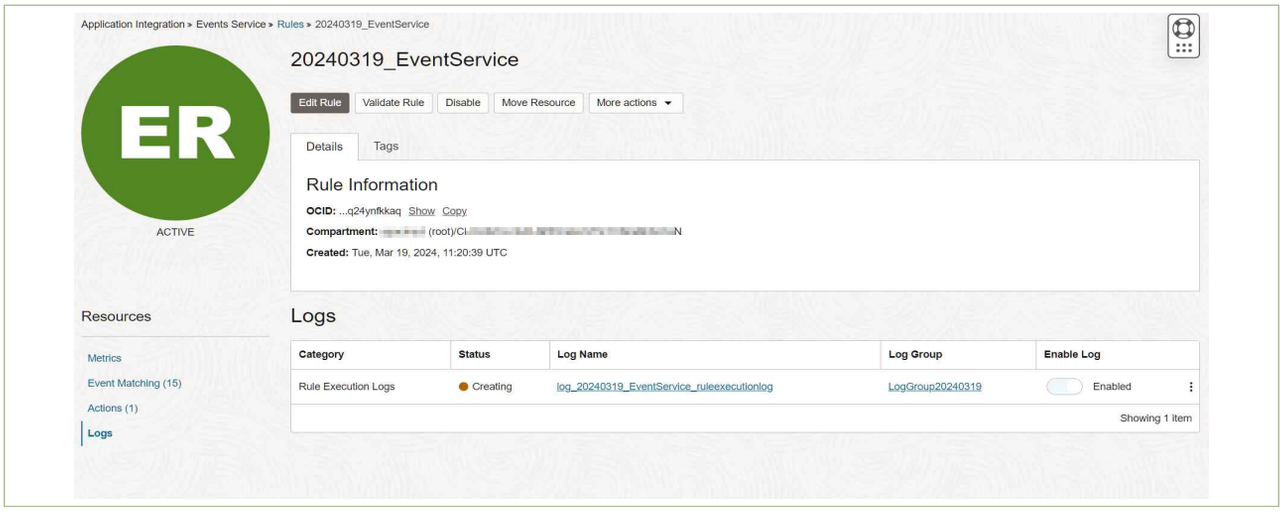
- (OCI 콘솔) '홈' → 'Observability & Management' → 'Events Service' → 'Create Rule'에서 Rule conditions → 'Condition' → 'Service Name' → 'Identity' → 'Event type' → 계정 변경 사항(생성, 삭제 등)에 대해 모니터링(Notification Email, SMS 등) 및 로깅 기능을 제공



| 그림 5.7.1 | 모니터링 리소스 지정(Service Name을 Identity로 설정)

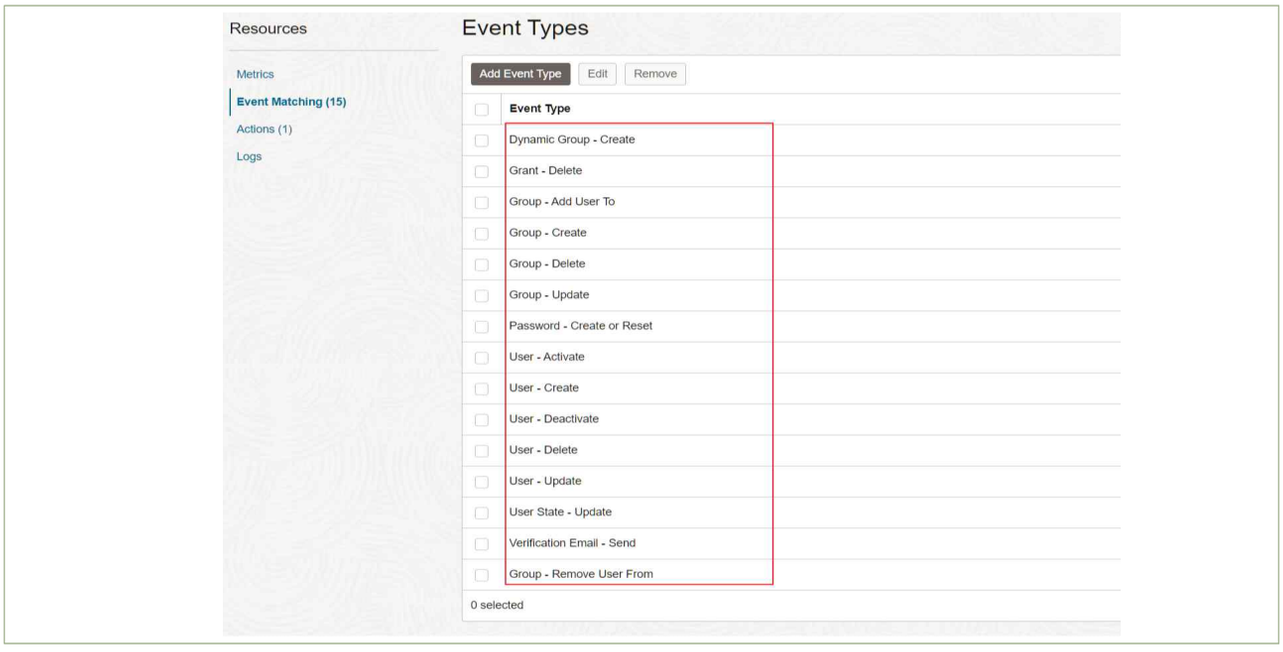


| 그림 5.7.2 | 모니터링 알람 설정



| 그림 5.7.3 | 행위 추적성 로깅 활성화

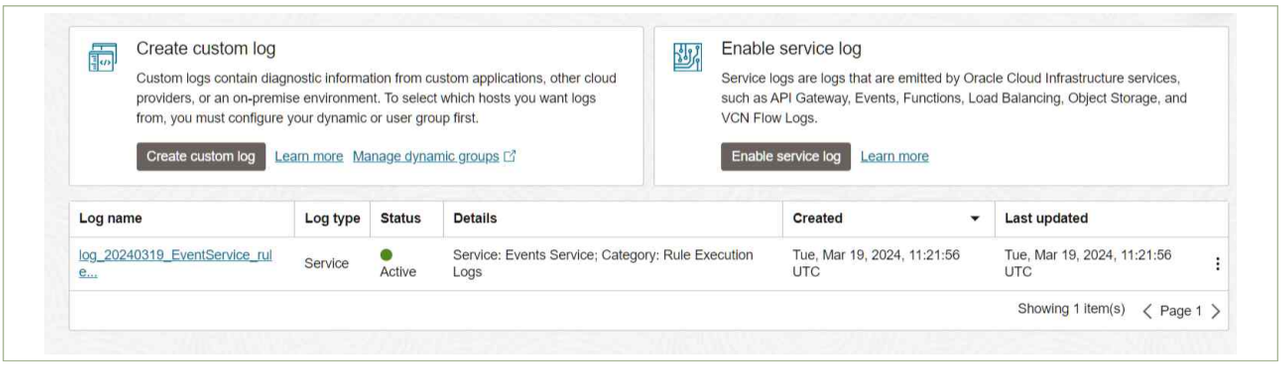
- 리소스 변경 사항의 행위 추적성은 Logs에 남겨 추후 지속적으로 검토할 수 있도록 제공
- Logs → Enable Log → 활성화 (로그 저장을 위해 Log Group 생성 필요)



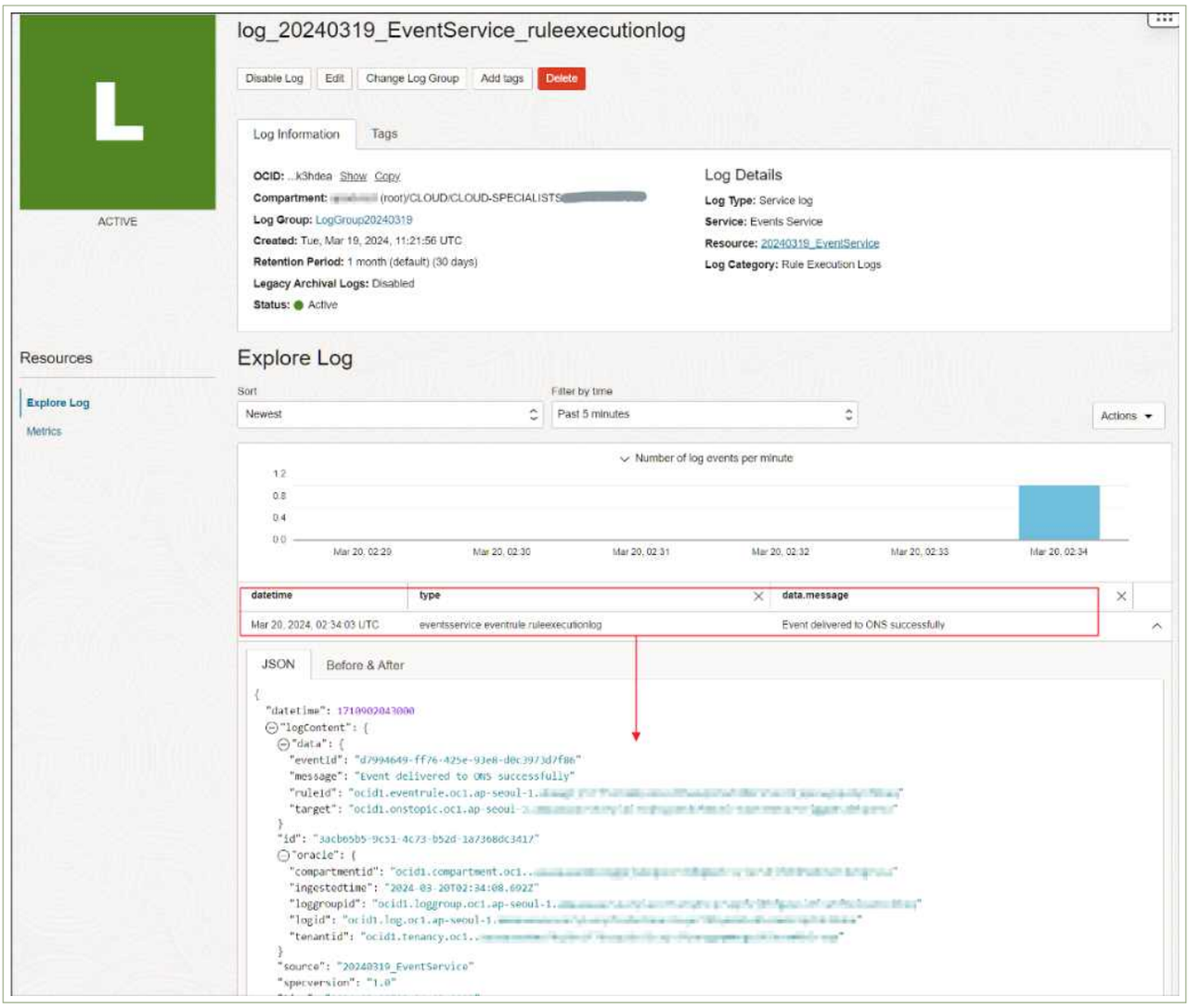
| 그림 5.7.4 | 행위 추적성 생성 확인

2) 전자금융감독규정 및 금융회사 내부 규정 등에 수립된 주기에 맞추어 주기적 검토 수행

- (OCI 콘솔) '홈' → 'Observability & Management' → 'Logging' → 'Logs' → '생성한 Log 선택'에서 계정변경, 네트워크 변경 등 다양한 보안 모니터링에 대한 주기적인 검토가 가능하도록 지원

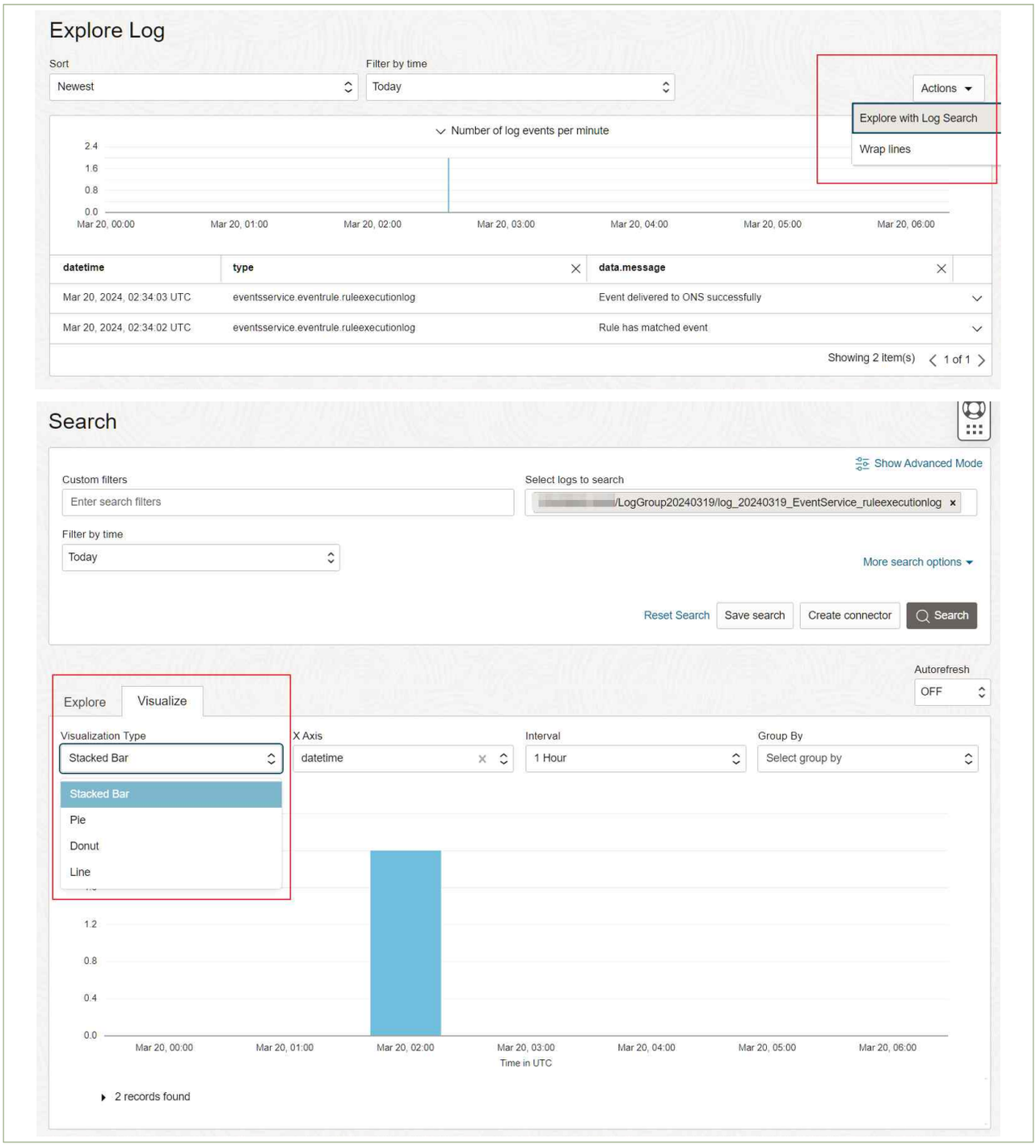


| 그림 5.7.5 | 변경 사항에 대한 로그 주기적 검토



| 그림 5.7.6 | 클라우드 리소스 행위 추적성 확인

- 검색된 로그에서 Action → Explore with Log Search → Explorer or Visualize를 선택하여 원하는 필드나 로그 생성 시간 등을 조회할 수 있는 기능을 제공



| 그림 5.7.7 | 로그 분석 기능 제공

4 참고 사항

- [Event Service] https://cloud.oracle.com/events/rules?region=ap-seoul-1
- [Logging] https://cloud.oracle.com/logging/logs?region=ap-seoul-1

6. API 관리

6.1. API 호출 시 인증 수단 적용
6.2. API 호출 시 무결성 검증
6.3. API 호출 시 인증 키 보호대책 수립
6.4. API 이용 관련 유니크 값 유효 기간 적용
6.5. API 호출 구간 암호화 저장

6 API 관리

1 기준

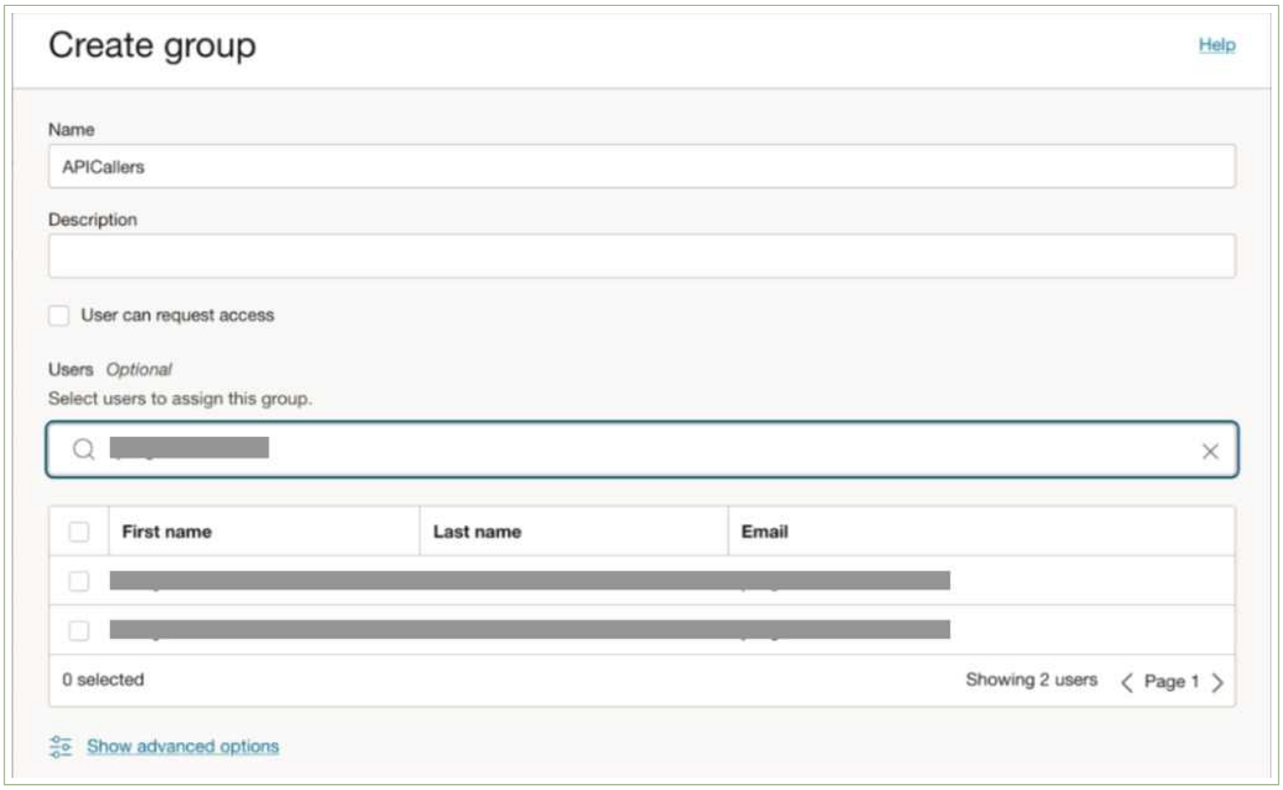
식별번호	기준	내용
6.1	**API 호출 시 인증 수단 적용**	클라우드 가상 자원 관리를 위한 API를 안전하게 호출하기 위한 인증 수단을 적용하여 보안성을 강화해야 한다.

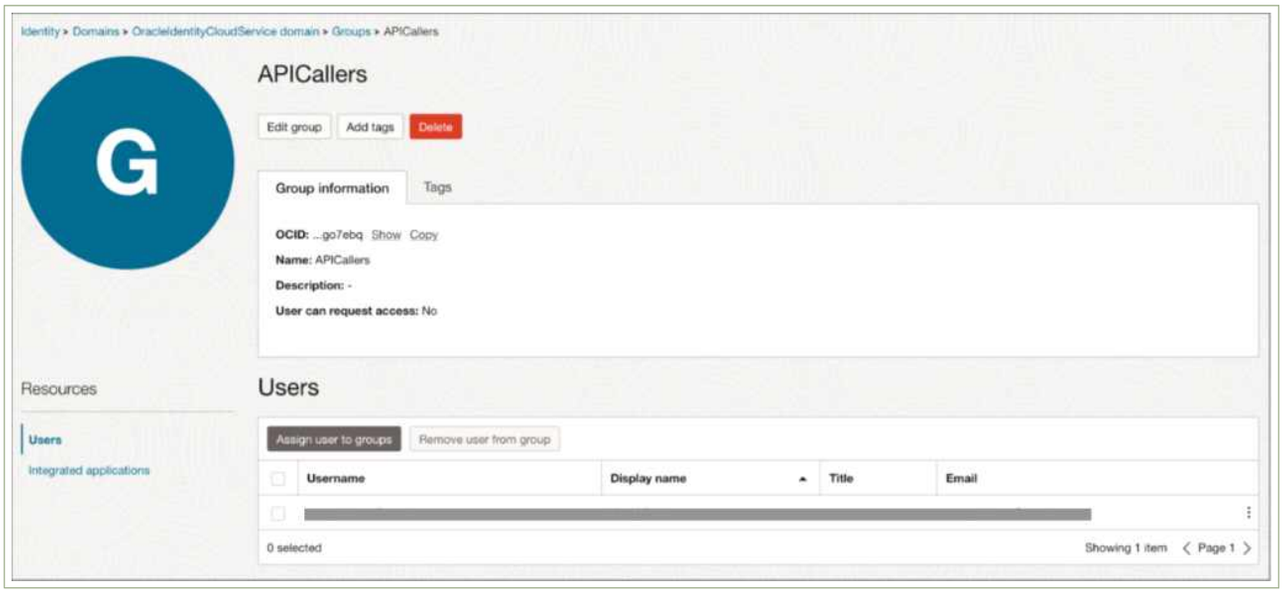
2 설명

- API 호출 시 이용자를 인증할 수 있는 수단을 적용하여야 한다.
  1) API 호출이 가능한 IP 지정 *(필수)*
  2) IAM 기능과 연동하여 API를 호출할 수 있는 권한을 제어
  3) API 호출 시 사용되는 인증값을 단기 인증값으로 사용 등

3 우수 사례

- (가상 자원관리시스템) '홈' → 'Identity & Security' → 'Identity' → 'Policies' → 'Create Policy'를 통해 사용자그룹에 API 호출 권한을 할당할 수 있음
  1) IAM 기능과 연동하여 API를 호출할 수 있는 권한 제어
     - API 호출을 위한 사용자 그룹을 생성(접근권한 할당)

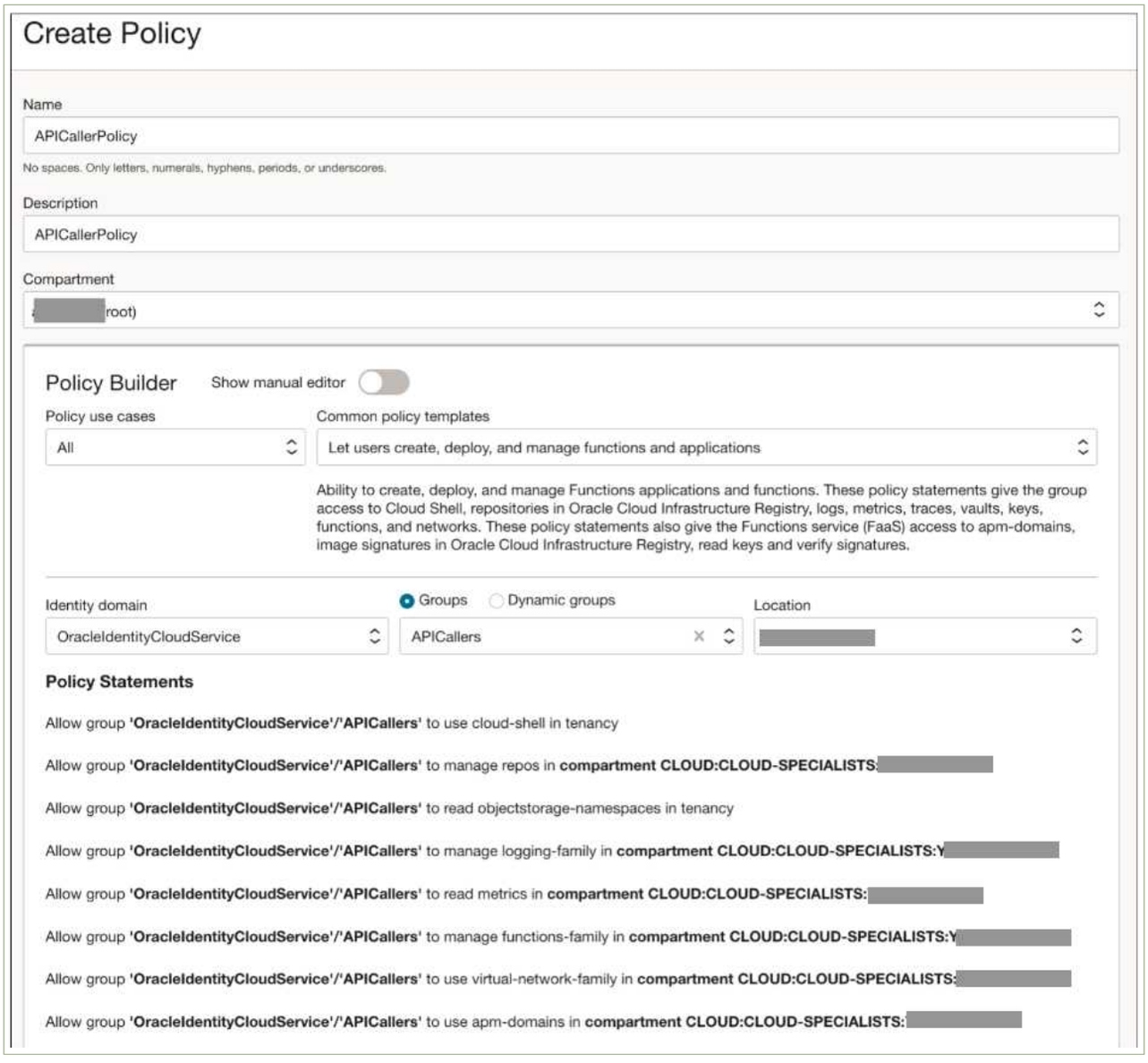




- 클라우드 가상 자원 관리를 위해 다음 링크와 같이 각 OCI 서비스에 대한 API를 제공하며, IAM Policy를 통해 사용자 그룹에 대한 자원 사용 권한 및 API 사용 권한을 제어
- IAM Policy Builder를 사용한 권한 설정 예시

  여러 서비스 중에 Compute 서비스에 대한 권한을 설정하는 경우, Policy Builder에서 Compute Instance 검색 후 Let users launch Compute instances를 선택하여 관련 권한을 설정

  필요하면 Show manual editor 클릭 후 '불필요한 정책을 제거'



- IAM 기능을 통해 API 호출 접근 권한을 할당한 정책 생성

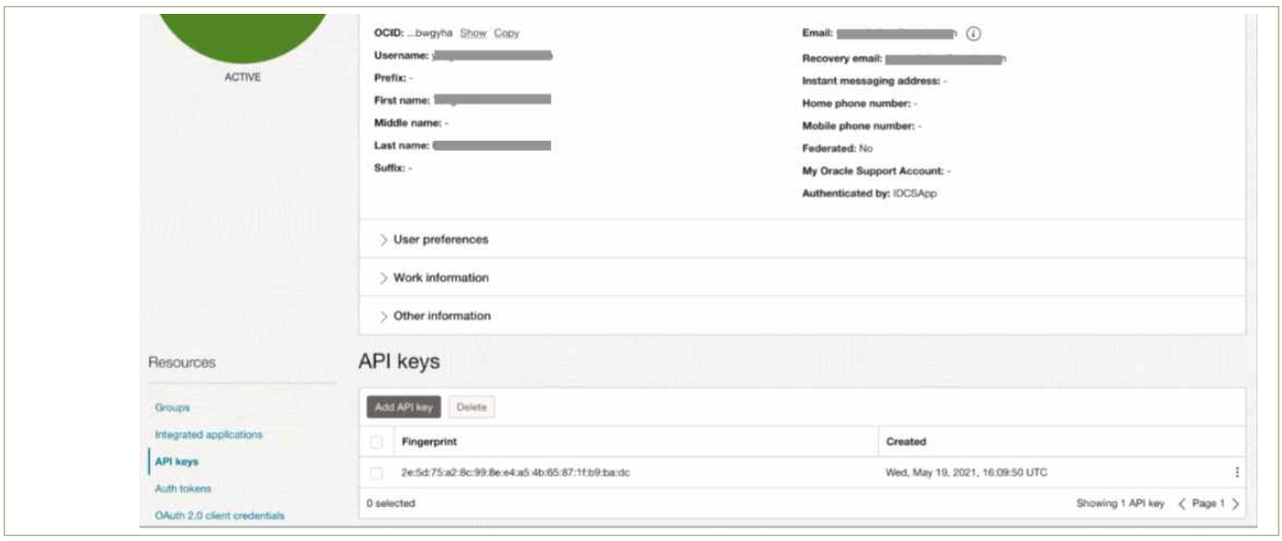
정책 예시(샘플)

분류	정책	조건
API Compute instance에 대한 호출	Allow group APICallers to manage instance-family in compartment MyCompartment Allow group APICallers to read instance-family in compartment MyCompartment	Manage instance-family : 인스턴스 생성, 종료, 재부팅 등 관리 작업 허용 Read instance-family : 인스턴스 목록 조회, 세부 정보 확인 허용
OCI Function에 대한 호출 권한	Allow group APICallers to use functions-family in compartment MyCompartment	use functions-family : Functions를 호출하고 실행할 수 있는 권한

- (가상 자원관리시스템) '홈' → 'Identity & Security' → 'Domains' → 'Users' → '사용자 선택' → 'API Keys' 를 통해 특정 사용자 또는 사용자 그룹에게만 API 호출 권한을 할당할 수 있음(API Gateway, Function 등)

2) API 호출 시 사용되는 인증값을 단기 인증값으로 사용 등

- Temporary Session Token, OCI의 세션 기반 인증으로 임시 자격 증명(IAM Federation, Instance Principal 또는 CLI를 통해 발급을 제공하며, 이 토큰은 몇 시간 동안만 유효(기본적으로 1시간, 최대 24시간)



- 생성된 API 키를 ~/.oci/config 파일에 추가

```
plantext
[DEFAULT]
user=ocid1.user.oc1..〈user_ocid〉
fingerprint=〈api_key_fingerprint〉
key_file=〈path_to_private_key〉
tenancy=ocid1.tenancy.oc1..〈tenancy_ocid〉
region=〈region〉
```

- 세션 토큰 발급

  〈region〉은 사용 중인 OCI 리전(예: South Korea Central(Seoul))

```
bash
oci session authenticate --region 〈region〉
```

- 브라우저에서 로그인하여 인증을 완료하면 CLI가 임시 세션 토큰을 생성하고,

  ~/.oci/config에 추가함

```
plantext
[TEMP_PROFILE] security_token_file=~/.oci/sessions/〈session_name〉/token
user=ocid1.user.oc1..〈user_ocid〉
fingerprint=〈api_key_fingerprint〉 tenancy=ocid1.tenancy.oc1..〈tenancy_ocid〉
region=〈region〉
```

- API 호출 예시 (예, Python sdk로 호출한다고 하면)

  세션 토큰을 사용하여 API 요청에 서명함

  --profile TEMP_PROFILE은 위에서 생성한 세션 토큰 프로파일을 참조

Python

```
import oci
# OCI 설정 로드
config = oci.config.from_file("~/.oci/config", "TEMP_PROFILE")
compute_client = oci.core.ComputeClient(config)
# 컴파트먼트 OCID
compartment_id = "<your_compartment_ocid>"
# 인스턴스 목록 조회
response = compute_client.list_instances(compartment_id=compartment_id)
instances = response.data
# 결과 출력
for instance in instances:
    print(f"Instance: {instance.display_name}, State: {instance.lifecycle_state}")
```

Text (출력 예시)

```
Instance: MyInstance1, State: RUNNING
Instance: MyInstance2, State: STOPPED
```

4 참고 사항

- OCI API Reference: https://docs.oracle.com/en-us/iaas/api/

1 기준

식별번호	기준	내용
6.2	**API 호출 시 무결성 검증**	클라우드 가상 자원 관리를 위한 API 호출 시 무결성을 보장하여야 한다.

2 설명

- API 호출 시 호출 메시지의 무결성을 보장하는 방안을 확보하여야 한다.
  1) API 보안 키와 서명을 통한 변조 방지 대책 마련 등

3 우수 사례

- 서명(Signature) 기반 인증 및 검증 방식
  1) OCI API는 무결성 검증은 주로 Authorization 헤더를 통해 이루어지며, API 개인 키와 RSA-SHA256 알고리즘을 통해 서명되어 요청의 진위 여부와 데이터 변조 방지를 보장함
     - API 서명(Signing)
       OCI API는 요청에 서명하여 무결성을 검증하며, 클라이언트는 비밀키(Private key)를 사용해 요청의 주요 요소를 기반으로 HMAC-SHA256 해시를 생성함. 이 해시는 Authorization 헤더에 포함되며, 서버는 공개키(Public key) 또는 API 키를 사용해 서명을 검증하여 요청이 변조되지 않았는지 확인함
     - Authorization 헤더 구성

```
Authorization: Signature
version="1",keyId="〈tenancy_ocid〉/〈user_ocid〉/〈key_fingerprint〉",
algorithm="rsa-sha256",signature="〈서명〉",headers="(request-target) host date ..."
```

     - OCI API 무결성 보장
       Request 핵심 요소(예: URL, 날짜, 페이로드)가 서명에 포함되므로, 중간에 데이터가 변경되면 서명이 일치하지 않아 요청을 거부하고, Date 헤더를 통해 요청의 유효 기간을 제한하여 재전송 공격(Replay Attack)을 방지함

단계	설명	무결성 보장 요소
1. 키 쌍 생성 및 등록	- 로컬 환경에서 RSA(2048/4096) 또는 ECDSA 키 쌍을 생성 - Public Key를 OCI 콘솔 → 사용자 → API Keys에 등록 - 등록 시 확인되는 **Fingerprint(지문)**과 사용자 OCID(ex: ocid1.user.oc1..aaaa...)가 연동	- 서버가 해당 Public Key로 "누가 서명했는지"를 식별하고 검증할 수 있음 - Private Key는 유출되지 않도록 안전하게 보관 필요
2. 헤더 준비	- 필수 헤더: date(또는 x-date), host - (POST/PUT 시) content-type, content-length, opc-content-md5 또는 x-content-sha256 등 - 바디 무결성 해시: 요청 바디 전체를 MD5/SHA-256으로 해싱 후 Base64로 삽입(Body 변조 방지)	- date를 통해 OCI가 5분 내 요청만 유효하게 처리 → Replay 공격 방지 - host는 실제 호출하는 도메인/엔드포인트와 일치해야 함 - opc-content-md5(또는 x-content-sha256)로 본문이 변조되지 않았음을 확인
3. 서명 문자열 구성	- 서명에 포함할 항목들을 정해진 순서로 문자열로 구성 ① HTTP 메서드 & 요청 경로(서비스에 따라 변동) ② date/x-date, host, 바디 해시 등 헤더 ③ 각 항목 사이에 개행 또는 특정 구분자 삽입 - 예시: POST /20160918/instances HTTP/1.1 date: Fri, 10 Apr 2025 12:34:56 GMT host: iaas.ap-seoul-1.oraclecloud.com content-type: application/json content-length: 349 opc-content-md5: d41d8cd98f00b204e9800998ecf8427e	- 헤더 + 바디 해시 + 메서드 정보를 모두 포함한 문자열에 서명 → 요청 전체 변조 여부를 확인 가능
4. 서명 생성	- 위에서 만든 문자열을 개인 키(Private Key)로 RSA 또는 ECDSA 서명 - 서명 결과를 Base64로 인코딩해서 문자열화 - 예: mZ5w/3AB...==	- 개인 키를 가지고 있는 사용자만 이 서명을 올바르게 생성 가능 → 인증(누가 보냈는지) + 무결성 보장
5. Authorization 헤더 설정	- 최종 요청 헤더에 다음과 같이 삽입: ```http Authorization: Signature version="1", keyId="ocid1.user.oc1..aaaaaaaa.../⟨fingerprint⟩", algorithm="rsa-sha256", headers="date host content-type content-length opc-content-md5", signature="mZ5w/3AB...==" ```	- keyId에는 사용자 OCID/키 지문 명시 - headers 필드는 실제 서명에 사용한 헤더 이름을 공백으로 구분 - 서버가 이 정보를 바탕으로 서명 검증
6. 서버(OCI) 검증	- 서버는 keyId(사용자 OCID + 키 지문) 기반으로 등록된 Public Key 조회 - 요청에 포함된 헤더 + 바디 해시로 서명 문자열 재구성 후, Public Key로 서명 유효성 검증 - date(or x-date)가 서버 시각 ±5분 내인지 확인	- 서명이 정상이어야 하며(무결성), 시간도 맞아야 함(Replay 방지). - 헤더나 바디가 하나라도 바뀌면 서명 검증에 실패 → 변조 방지

4 참고 사항

- https://docs.oracle.com/en-us/iaas/Content/API/Concepts/usingapi.htm
- https://docs.oracle.com/en-us/iaas/Content/API/Concepts/signingrequests.htm#Request_Signatures

1 기준

식별번호	기준	내용
6.3	**API 호출 시 인증 키 보호 대책 수립**	API 호출 시 인용되는 유니크 값(ex. 보안 키 등)은 안전하게 보관 및 관리하여야 한다.

2 설명

- API 호출 시 인용되는 유니크 값(ex. 보안 키 등)은 안전하게 보관 및 관리하여야 한다.
  1) API 호출에 서명하는 데 사용되는 비밀 키, 인증서 등은 노출되지 않도록 관리하여야 한다. (CSP 사업자에서는 최초 API 보안 키가 생성될 때 보호 방안을 작성할 필요가 있음)

3 우수 사례

- (가상 자원관리시스템) '홈' → 'Identity & Security' → 'Vault' → 'Create Vault'에서 Vault를 생성하고, Vault 내 Secret 섹션으로 이동하여 비밀을 생성하여, IAM을 통해 접근할 수 있는 사용자, 그룹 또는 리소스를 제한함
  1) OCI Vault 사용

  OCI Vault는 OCI에서 제공하는 관리형 서비스로, 비밀 키, 암호, 인증서, API 키 등의 민감 정보를 중앙에서 안전하게 저장하고 수명 주기를 관리할 수 있게 해줍니다.

  (1) 작동 방식
  - OCI Vault에 비밀(Secret) 리소스를 생성하고, 여기에 .pem 개인 키 파일의 내용을 저장합니다.
  - API를 호출해야 하는 애플리케이션(또는 Compute Instance, Function 등)의 IAM 정책에 해당 Vault의 특정 '비밀'을 읽을 수 있는 권한만 부여
  - 애플리케이션은 OCI SDK를 통해 Vault에서 직접 비밀 키를 메모리로 읽어와서 사용

  (2) 장점
  - 최고 수준의 보안: FIPS 140-2 Level 3 인증을 받은 HSM(하드웨어 보안 모듈)으로 키를 보호
  - 중앙 관리 및 감사: 모든 비밀 정보 접근에 대한 로그가 기록되어 추적하기 용이
  - IAM 통합: OCI의 강력한 IAM 정책을 통해 세분화된 접근 제어가 가능
  - 자동 교체: 키 교체 주기를 설정하고 자동화 가능

4 참고 사항

- OCI Vault (OCI 인스턴스 주체와 Vault를 사용하여 Secret 조회)
- https://www.ateam-oracle.com/post/using-the-oci-instance-principals-and-vault-with-python-to-retrieve-a-secret

1 기준

식별번호	기준	내용
6.4	**API 이용 관련 유니크값 유효기간 적용**	클라우드 가상 자원 관리를 위해 API 기능 이용 시, 세션 유효 기간 및 유니크 값(보안키 등)에 대한 만료기간을 설정하여야 한다.

2 설명

- API 세션 및 서명 값에 대한 유효 기간 설정하고, 유니크 값(보안 키 등) 유출 방지 대책으로 만료 기간을 적용하여야 한다.
  1) API 호출 세션의 유효 기간 설정
  2) 서명의 유효 기간 확인
  3) API 보안 키 만료 기간 설정
  4) 유니크 값(보안 키 등) 폐기 및 재발급 기능으로 만료 기간 준수 등

3 우수 사례

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Policies' → 'Create Policy'를 통해 사용자그룹에게 API 호출 권한을 할당할 수 있음
  1) API 호출 세션의 유효 기간 설정

     API 호출 세션의 유효 기간을 직접적으로 설정하는 기능은 현재 제공되지 않음

     OCI의 API 인증 매커니즘은 서명 기반(Signature-Based) 방식을 사용하며, 이 방식 자체가 세션의 유효성을 보장하는 특정 시간 제약을 포함
     - Request Signature Timestamp (요청 서명 타임스탬프)
       - 각 API 요청마다 서명을 통해 유효성을 검증합니다. 이 서명의 유효 기간은 OCI의 내부 보안 정책에 의해 5분으로 제한됨
       - OCI API 호출 시 HTTP 요청 헤더에 x-date 또는 date 필드에 포함되는 타임스탬프로 요청의 생성 시간 확인 가능
  2) 서명의 유효 기간 확인

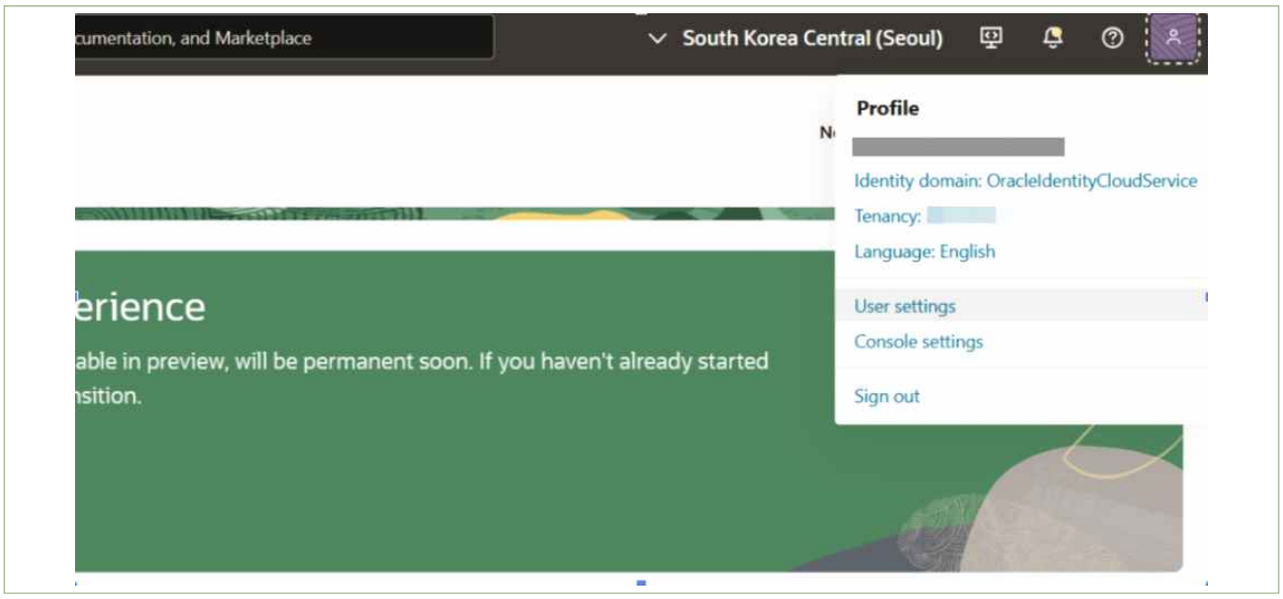
     [토큰 기반 인증과 세션 유효 기간 설정]
     - OCI CLI 또는 SDK에서 토큰 기반 인증(예: oci session authenticate)을 사용할 경우, 세션 토큰의 유효 기간을 설정할 수 있음

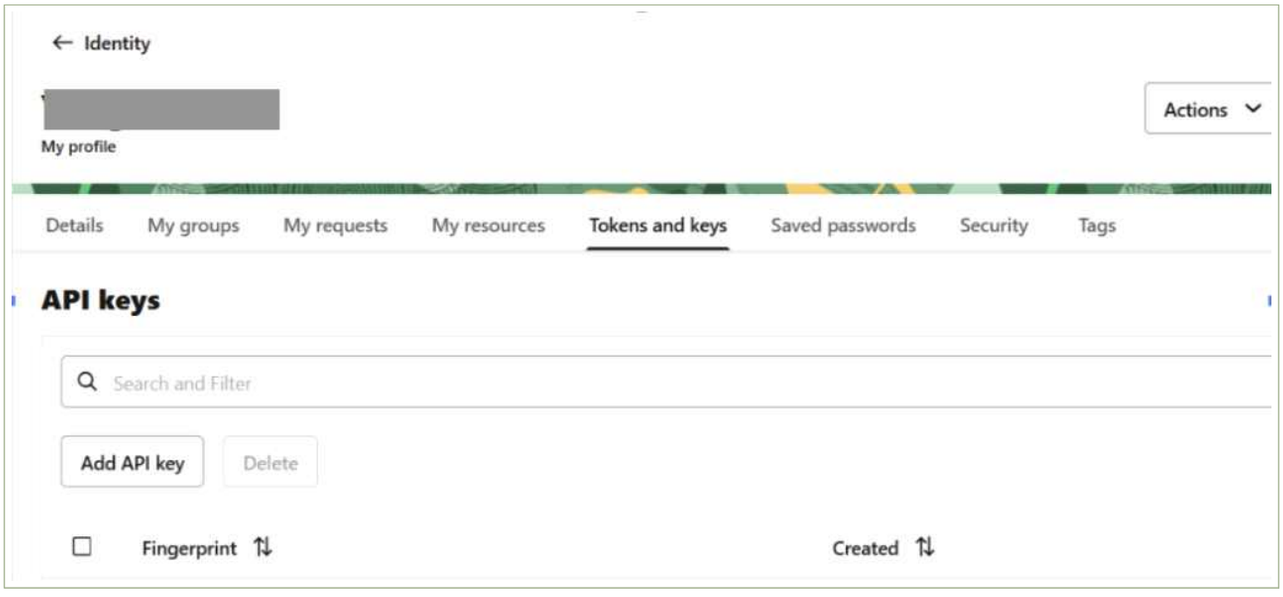
- 기본값은 60분이며, --session-expiration-in-minutes 파라미터를 통해 5분에서 60분 사이로 유효 기간 설정 가능

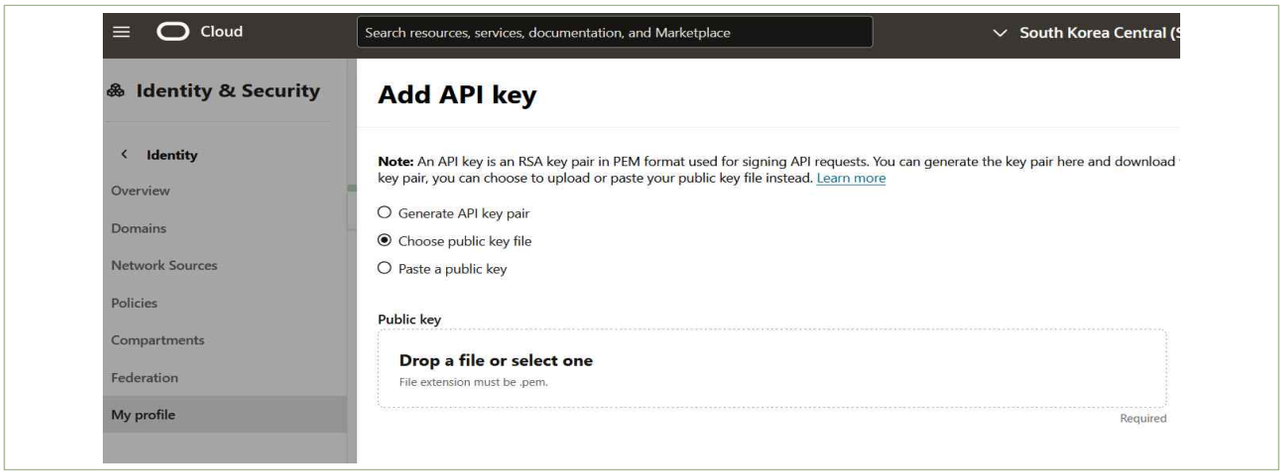
예) oci session authenticate --session-expiration-in-minutes 30

3) API 보안 키 만료 기간 설정

- (OCI 콘솔) '홈' → 'Profile' → 'User Settings' → 'Tokens and keys' → 'API Keys'를 통해 기존 API 키를 삭제하고, 새 공개 키를 업로드
- OCI API 서명 키 자체에는 만료 기간이 없지만, 보안 강화를 위해 주기적으로 키를 교체하고 IAM 정책으로 접근을 제한하는 것을 권장하며, 키 교체는 OCI 콘솔에서 새로운 공개 키를 업로드하고 구성 파일을 업데이트하는 방식으로 진행 가능



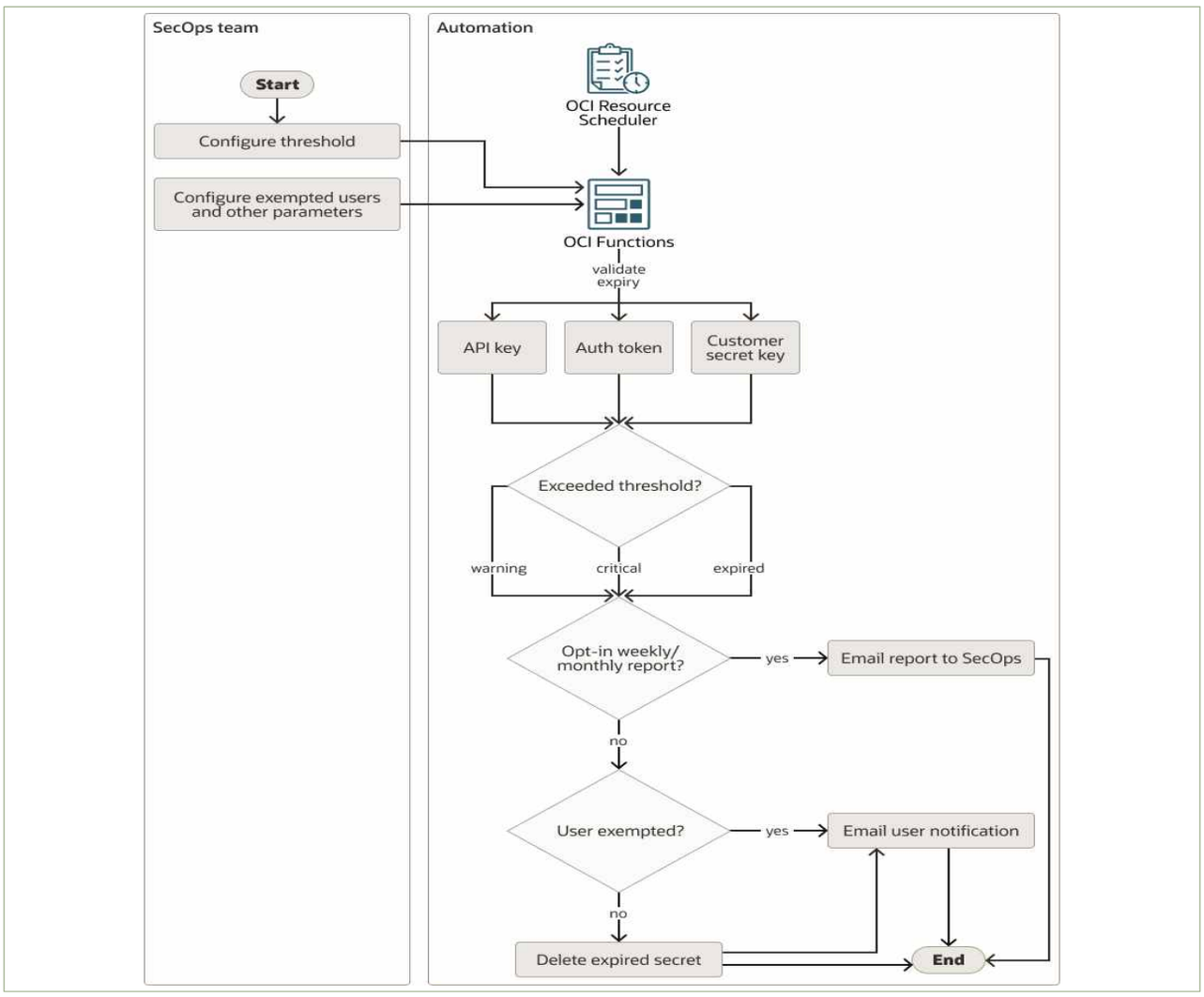




- 간접적인 만료 제어 방법

  자동화 스크립트: OCI Functions 또는 외부 스크립트를 사용하여 API 키의 생성, 삭제, 교체를 자동화할 수 있음

  * 구현에 필요한 절차는 아래 흐름도 참조



<table>
<tr><th>분류</th><th>내용</th></tr>
<tr><td>OCI SDK 설치</td><td>pip install oci</td></tr>
<tr><td>OCI 구성파일 설정</td><td>~/.oci/config 파일에 OCI 인증 정보(Tenancy OCID, User OCID, API 키, Region 등)를 설정
ini
[DEFAULT]
user=ocid1.user.oc1..〈user_ocid〉
fingerprint=〈key_fingerprint〉
key_file=~/.oci/oci_api_key.pem
tenancy=ocid1.tenancy.oc1..〈tenancy_ocid〉
region=ap-seoul-1</td></tr>
<tr><td>필요한 권한</td><td>IAM 정책으로 API 키 관리 권한 부여
Planintext
Allow group 〈your-group〉 to manage users in tenancy
Allow group 〈your-group〉 to manage api-keys in tenancy</td></tr>
<tr><td>샘플 Python 스크립트</td><td>Python
import oci
import datetime
from oci.identity import IdentityClient
import os

OCI 설정 로드
config = oci.config.from_file("~/.oci/config", "DEFAULT")
identity_client = IdentityClient(config)

대상 사용자 OCID (환경 변수 또는 하드코딩)
user_ocid = "〈target_user_ocid〉"

1. 기존 API 키 목록 조회
def list_api_keys():
    return identity_client.list_api_keys(user_ocid).data

2. 기존 API 키 삭제
def delete_api_key(key_id):
identity_client.delete_api_key(user_ocid, key_id)
print(f"Deleted API key: {key_id}")

3. 새 API 키 생성
def create_api_key():
    # 새 키 쌍 생성 (로컬에서 생성 후 공개 키 업로드)
key_file = "new_api_key.pem"
public_key_file = "new_api_key_public.pem"

    # OpenSSL 명령어로 키 생성 (실제로는 subprocess로 실행 가능)
    os.system(f"openssl genrsa -out {key_file} 2048")
    os.system(f"openssl rsa -pubout -in {key_file} -out {public_key_file}")
    with open(public_key_file, "r") as f:
        public_key = f.read()</td></tr>
</table>

<table>
<tr><th>분류</th><th>내용</th></tr>
<tr><td></td><td>Python
<pre>
    # API 키 업로드
    response = identity_client.upload_api_key(
        user_ocid, oci.identity.models.CreateApiKeyDetails(key=public_key)
)
    print(f"Created new API key: {response.data.id}")
    return response.data

4. 메인 로직
def rotate_api_keys():
    # 기존 키 조회
    api_keys = list_api_keys()

    # 90일 이상 된 키 삭제 (예: 생성일 기준)
    for key in api_keys:
        created_date = key.time_created
        if (datetime.datetime.now(datetime.timezone.utc) - created_date).days > 90:
            delete_api_key(key.id)
    # 새 키 생성
    new_key = create_api_key()
    # 필요시 새 키를 Vault에 저장하거나 알림 전송 (별도 구현 필요)
    print("API key rotation completed.")
if __name__ == "__main__":
    rotate_api_keys()
</pre></td></tr>
<tr><td>스크립트 실행 및 스케줄링</td><td>터미널에서 스크립트 실행
bash
Python rotate_api_keys.py</td></tr>
<tr><td>OCI Functions로 자동화</td><td>1. OCI Functions 설정
- OCI Functions 서비스에서 Python 런타임으로 새 Function 생성
- 위 스크립트를 Function 코드로 업로드
- 필요한 환경 변수(예: user_oicd) 설정
2. 스케줄링
- OCI Events와 OCI Resource Scheduler를 사용해 주기적 실행(예: 매 90일) 설정
- 예: Event Rule로 “매 3개월마다 트리거” 설정 후 Function 호출
또는 외부 스케줄링 이용
Crontab: crontab으로 스크립트 실행 스케줄링도 가능함</td></tr>
</table>

3) 유니크 값(보안 키 등) 폐기 및 재발급 기능으로 만료 기간 준수 등

- 만료 기간 설정: 오라클 클라우드는 API 키 자체에 대해 자동 만료 설정 기능 부재, 생성 후 90일 뒤에 자동으로 만료되도록 지정하는 등의 기능은 제공되지 않음
- 오라클 클라우드 콘솔 또는 API를 통해 API 키를 언제든지 삭제(폐기) 또는 재발급(새로운 API 키 생성) 가능

4 참고 사항

- Required Headers – API 서명 키
- https://docs.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm#Required_Headers

1 기준

식별번호	기준	내용
6.5	**API 호출 구간 암호화 적용**	클라우드 가상 자원 관리를 위한 API 호출 시 암호화된 통신구간을 적용하여야 한다.

2 설명

- API를 통한 클라우드 가상 자원 관리 수행 시 네트워크 트래픽 보호를 위한 암호화된 통신구간을 적용하여야 한다.
  1) SSL 적용(ex. TLS 1.3)

3 우수 사례

- SSL 적용 : OCI API 요청은 HTTPS와 SSL Protocol TLS 1.3 미지원

7. 스토리지 관리

7.1. 스토리지 접근 관리
7.2. 스토리지 권한 관리
7.3. 스토리지 업로드 파일 제한

7 스토리지 관리

1 기준

식별번호	기준	내용
7.1	**스토리지 접근 관리**	스토리지 목적에 따라 외부 공개 차단 등 적절한 접근통제를 수행하여야 한다.

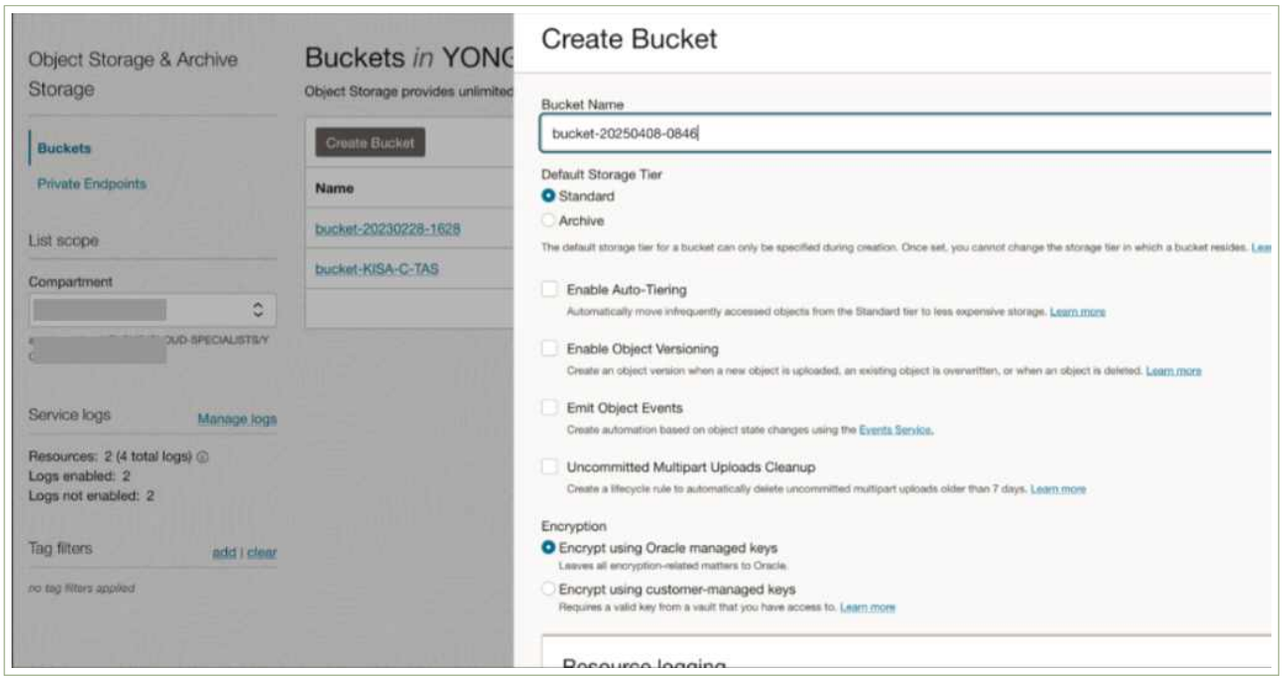
2 설명

- 스토리지 목적에 따라 외부 공개 차단 등 적절한 접근통제를 수행하여야 한다.
  1) 외부에 공개가 필요 없는 스토리지에 대해서는 퍼블릭 액세스 차단 등 방안 적용
  2) 스토리지 종류별 접근 가능한 계정 관리 수행(IAM 기능 등을 활용)
  3) 단축 URL 등 서명 값이 포함된 URL로 접근 시 통제 방안 수립(접근 가능 시간, IP 제어 등) 등 PAR 접근 권한

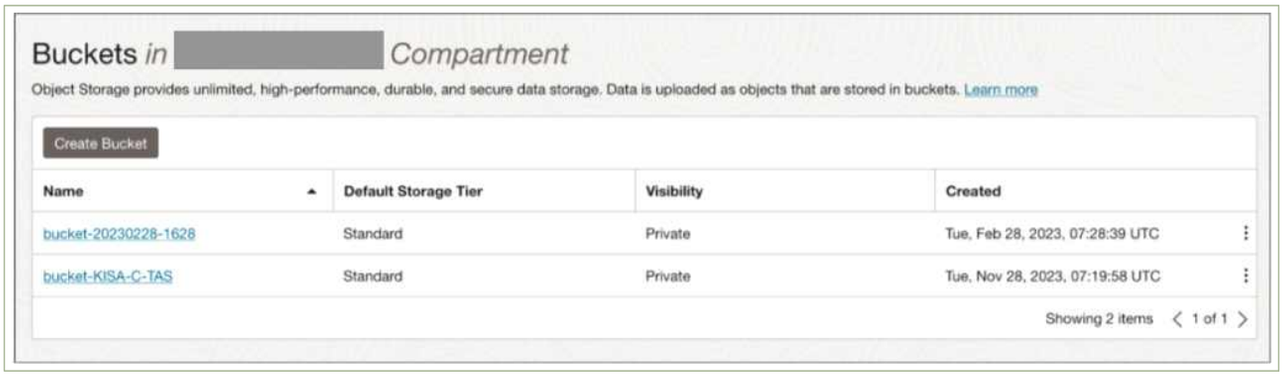
3 우수 사례

- (OCI 콘솔) '홈' → 'Storage' → 'Object Storage & Archive Storage' → 'Buckets' → 'Create Bucket에서 버킷 스토리지 생성(Default: Private)
  1) 외부에 공개가 필요 없는 스토리지에 대해서는 퍼블릭 액세스 차단 등 방안 적용
     - 버킷 스토리지 생성 시 Private 상태로 생성되며, OCI Cloud Guard를 통해 Public 상태로 변경 시 탐지 및 관리자에게 통보할 수 있음(외부에 공개하는 스토리지가 아닐 경우 Public 상태로 변경하더라도 강제로 Private 상태로 자동 변경 정책도 적용할 수 있음)

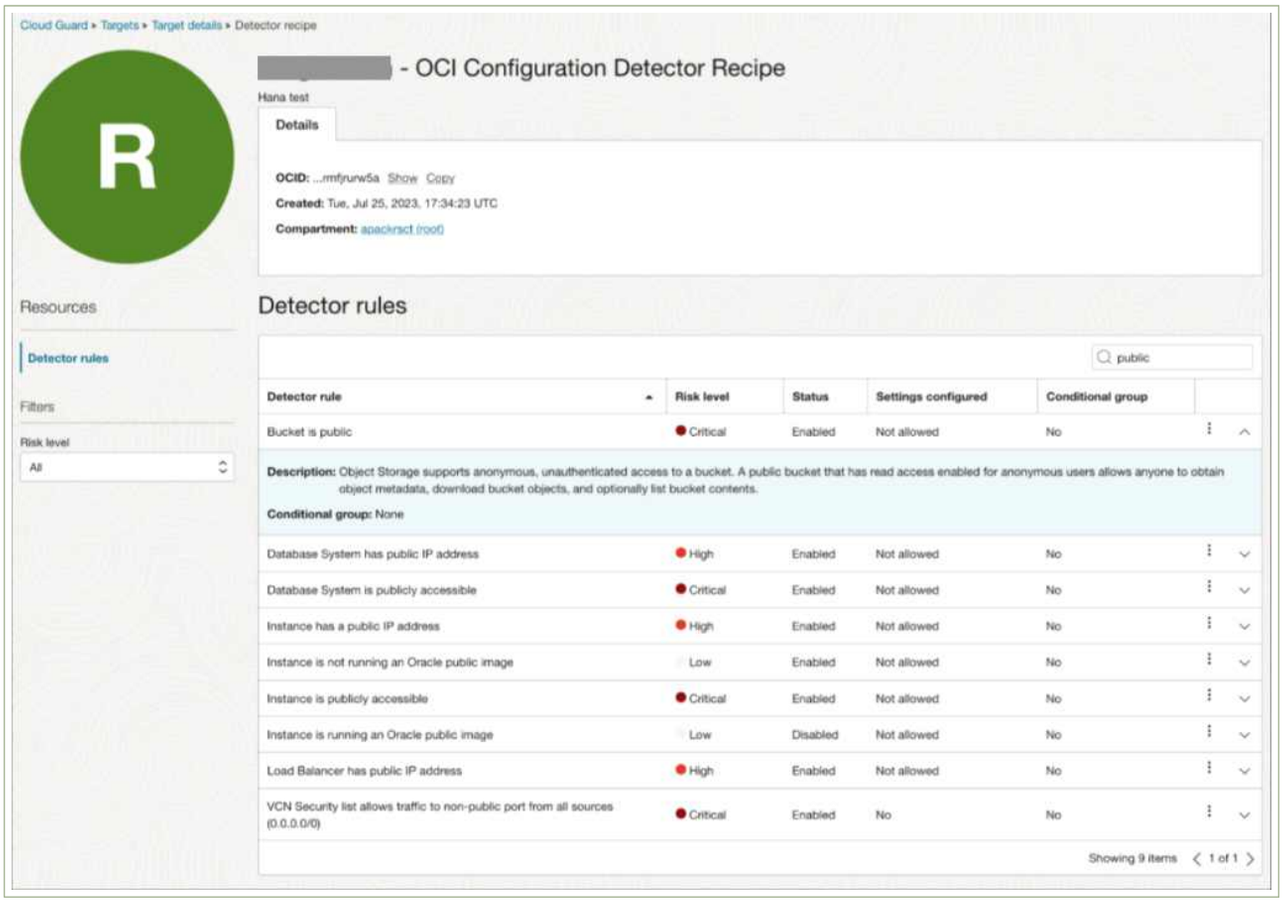
- 버킷 스토리지 생성



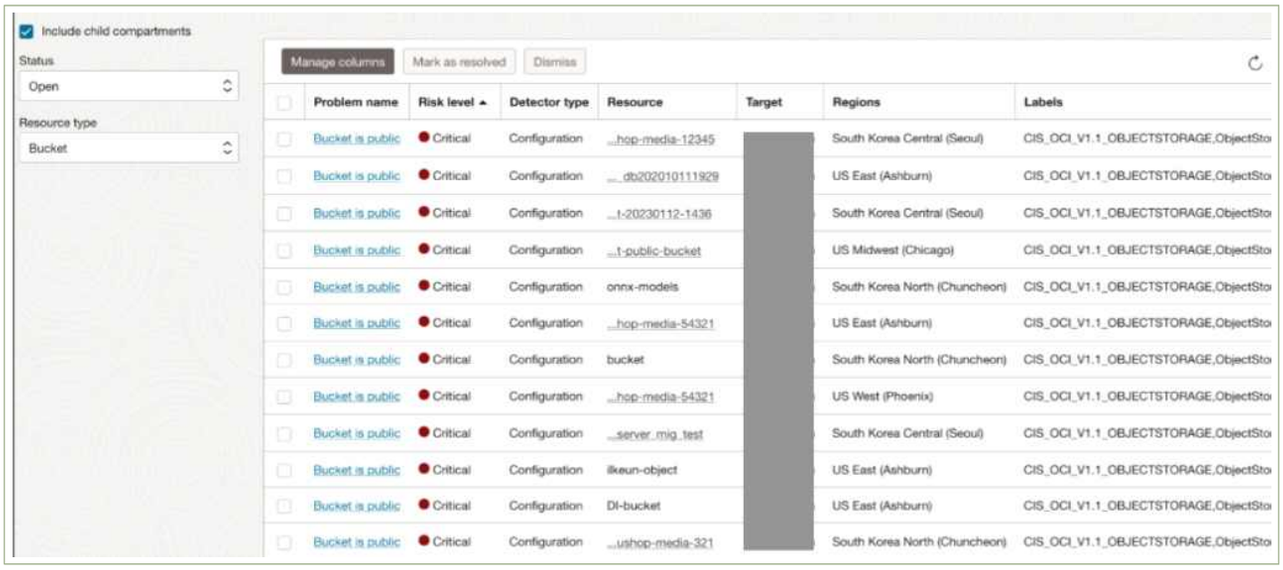
- 생성된 버킷 스토리지 상태(Private)



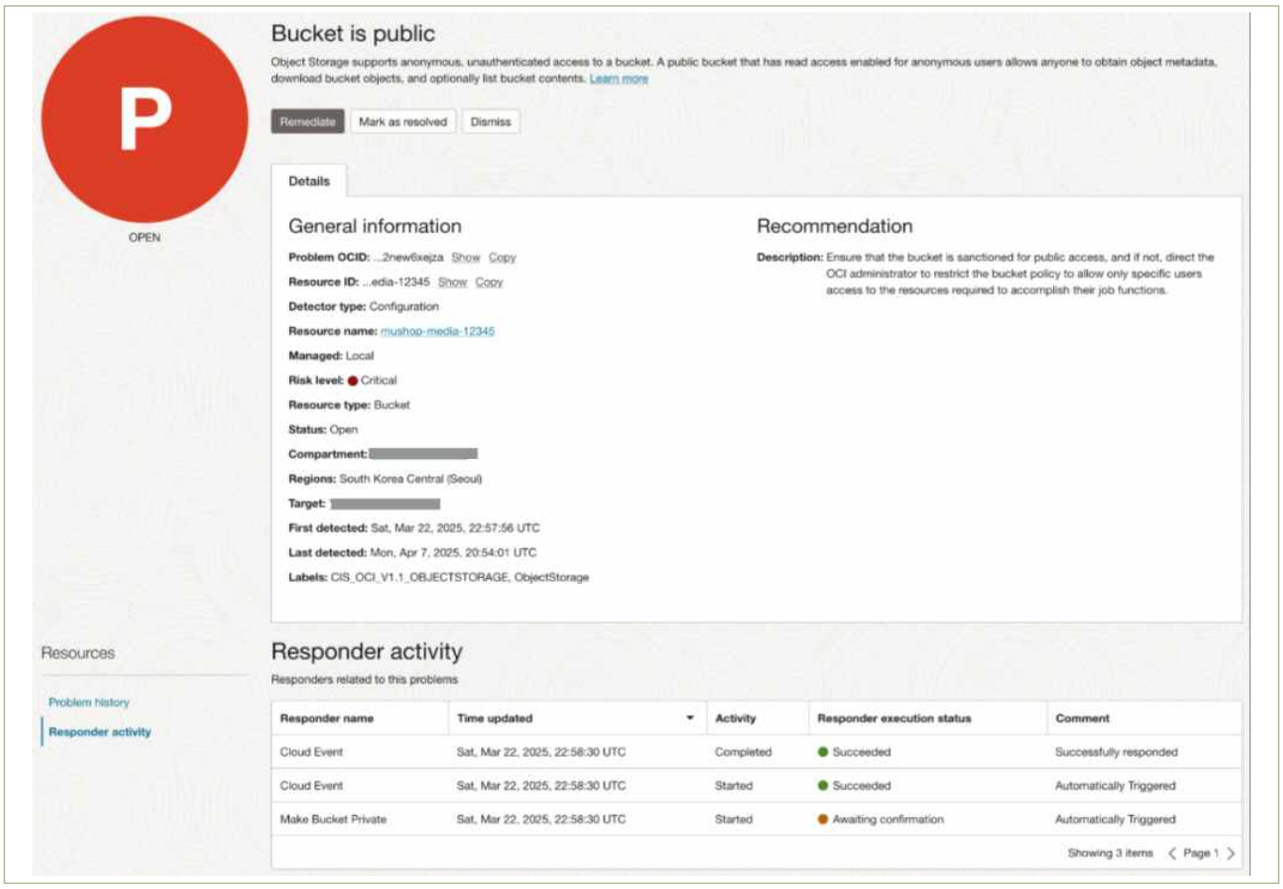
- Public 상태인 버킷 스토리지의 모니터링을 통해 실시간 확인 및 관리자 알림 설정
  OCI Cloud Guard, Configuration Detector Recipe



- OCI Cloud Guard를 통해 식별된 Public bucket 목록



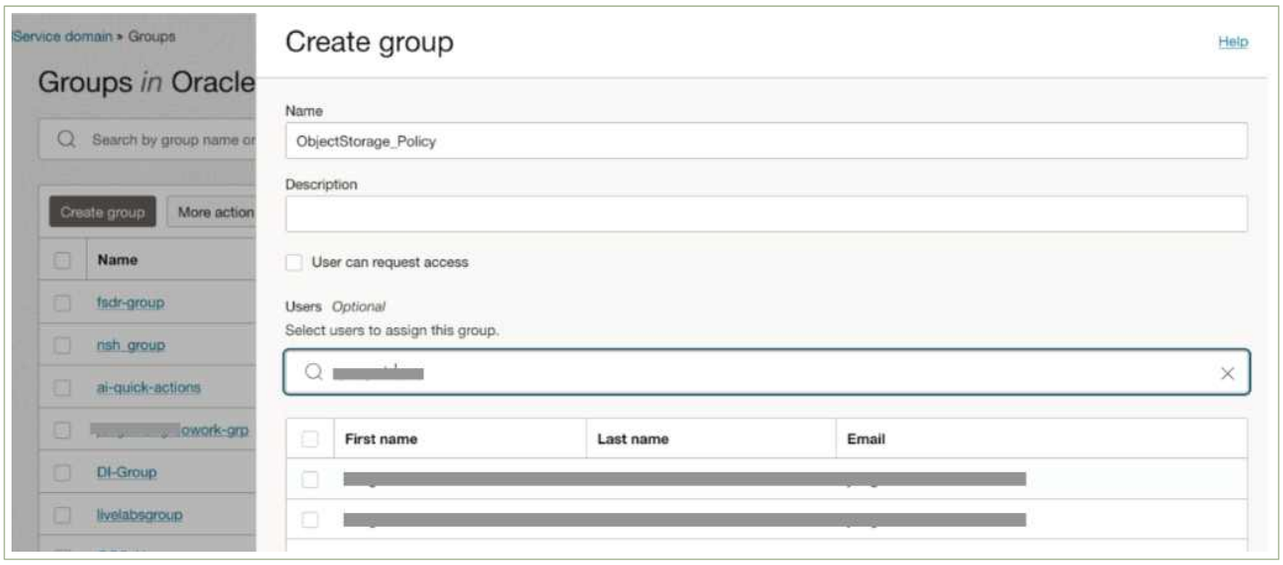
- 기업 내부 보안정책에 따라 모든 버킷을 Private 상태로 유지하기 위해서 내부 사용자가 Public 상태로 변경하더라도 강제로 Private 상태로 강제 변경 가능함
  Responder activity의 내용은 Cloud Guard, Responder recipe에 따라 강제 변경된 버킷 스토리지 이력을 확인할 수 있음



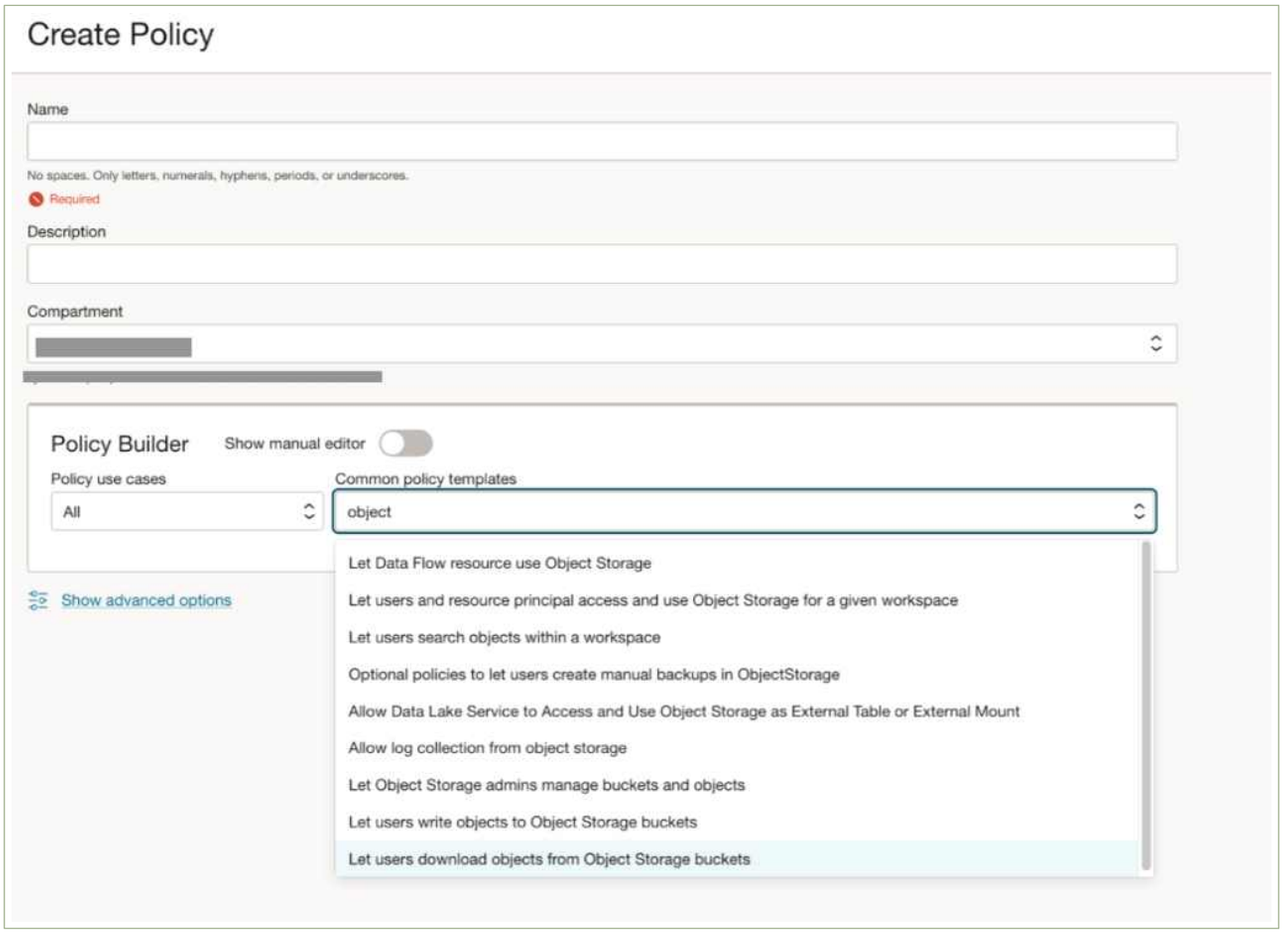
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Identity' → 'Policies' → 'Create Policy'에서 Object storage에 접근할 사용자 또는 사용자 그룹을 생성하고, 지정된 컴파트먼트 내 버킷을 읽기/쓰기 등 권한을 허용하는 정책을 적용

2) 스토리지 종류별 접근 가능한 계정 관리 수행(IAM 기능 등을 활용)

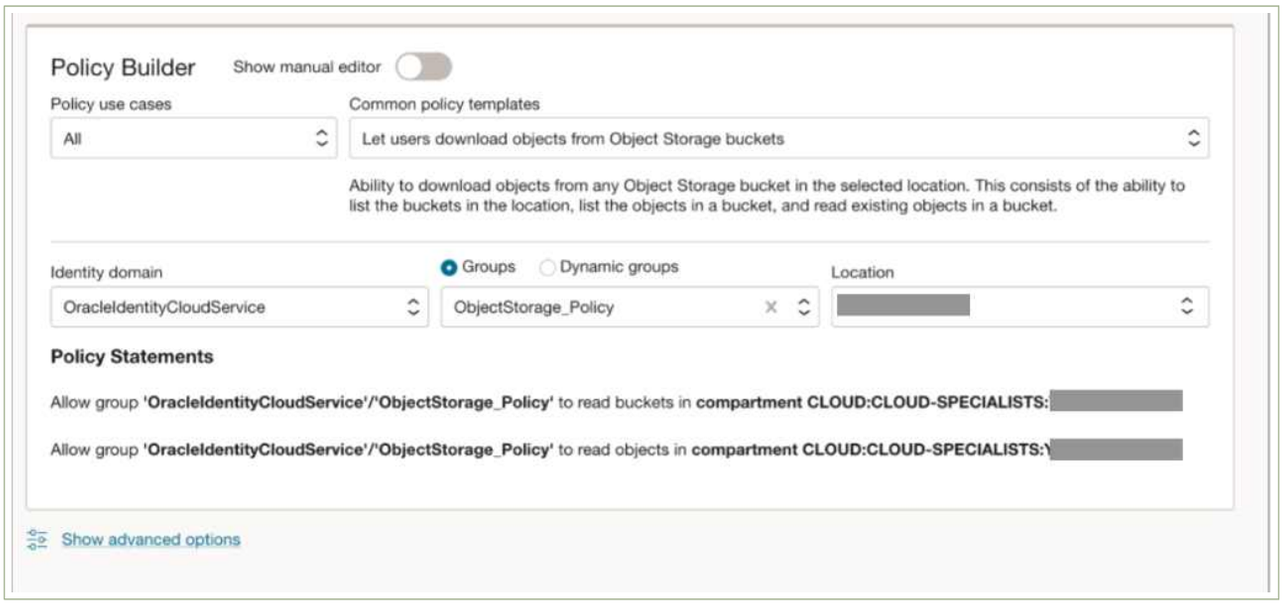
- 블록, 파일, 오브젝트 스토리지 모두 아래 절차에 따른 접근권한 설정 가능
- 사용자 그룹 생성 및 사용자 지정



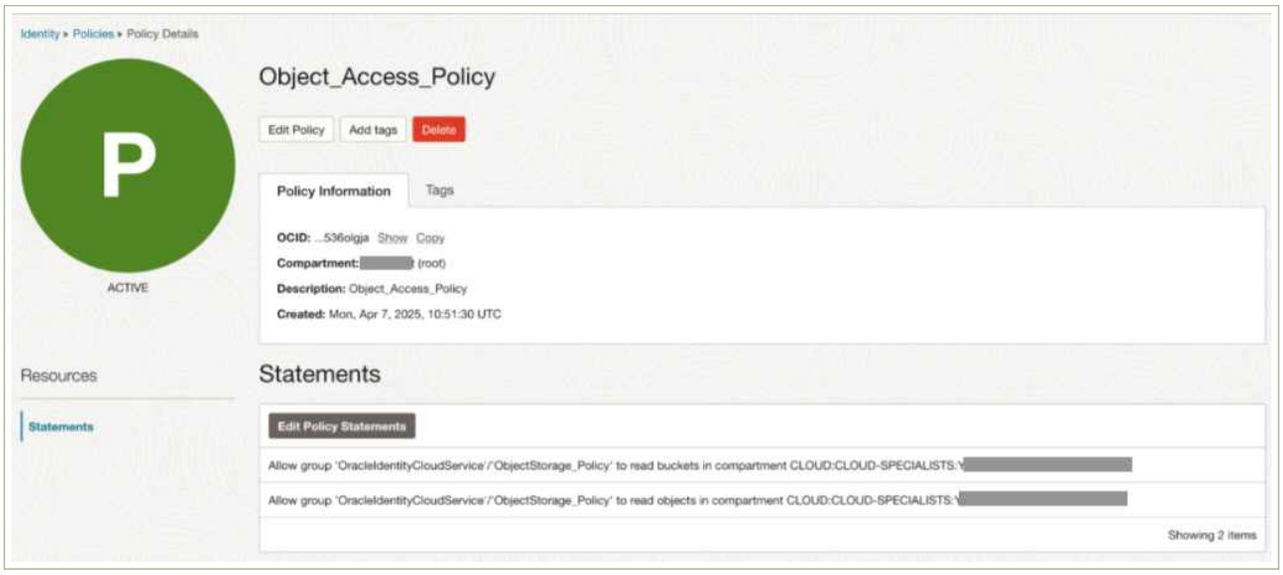
- Policy Builder, Common policy templates에서 object로 검색하여 다양한 정책을 선택할 수 있음



- 미리 생성한 사용자그룹(사용자지정)에 지정된 컴파트먼트 내 오브젝트 스토리지 버킷에서 객체(파일)을 다운로드 가능하도록 허용하는 정책 지정



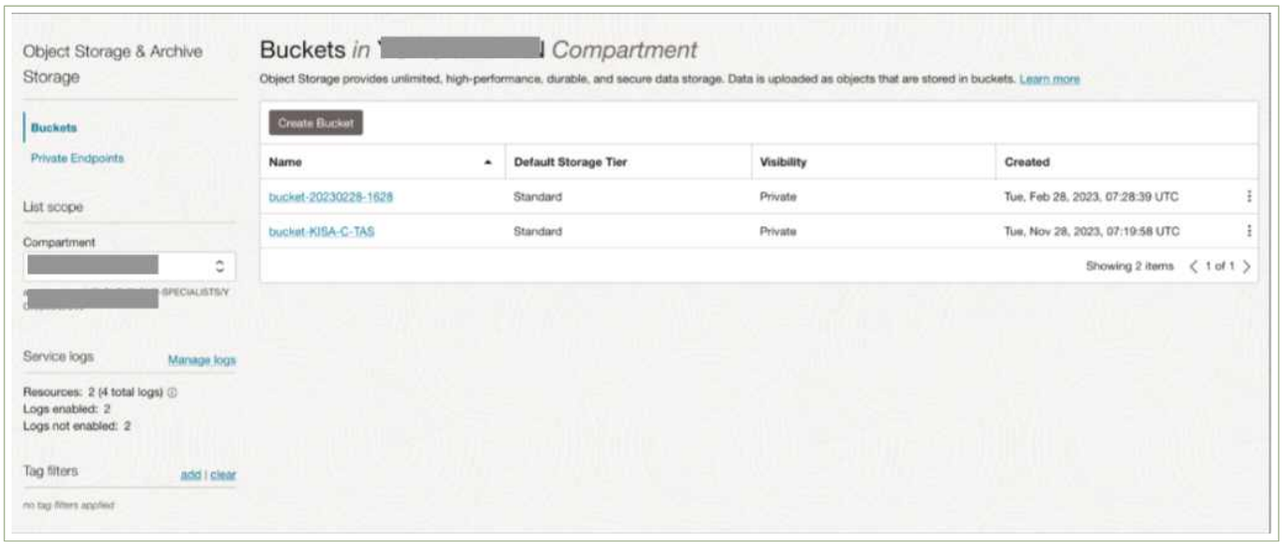
- 완료된 스토리지 접근권한 설정 내용



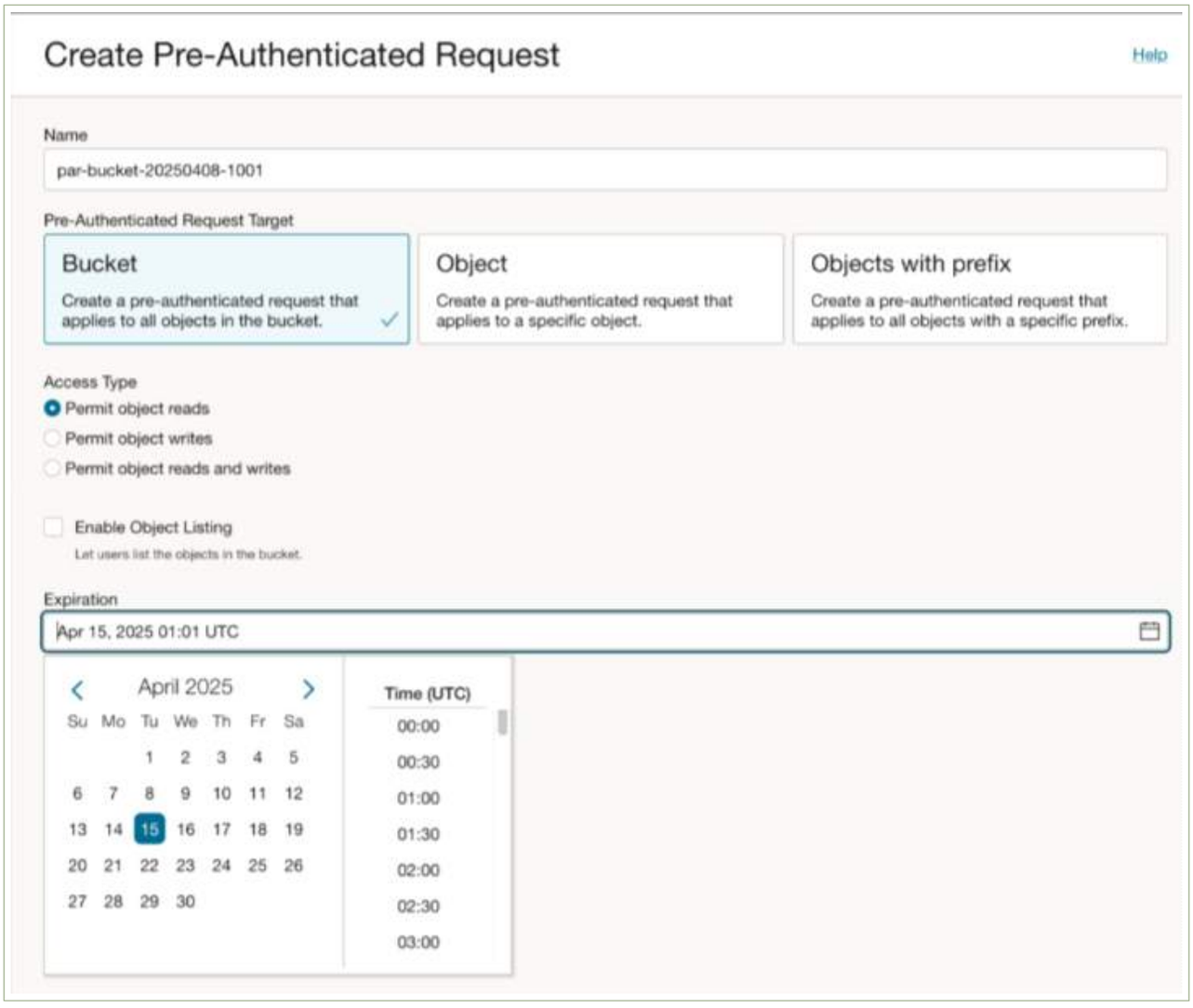
- (OCI 콘솔) '홈' → 'Storage' → 'Object Storage & Archive Storage' → 'Buckets' → 'Bucket' 선택 → 'Pre-Authenticated Requests' → 'Create Pre-Authenticated Request'에서 통제 방안 설정

3) 단축 URL 등 서명 값이 포함된 URL로 접근 시 통제 방안 수립(접근 가능 시간, IP 제어 등)

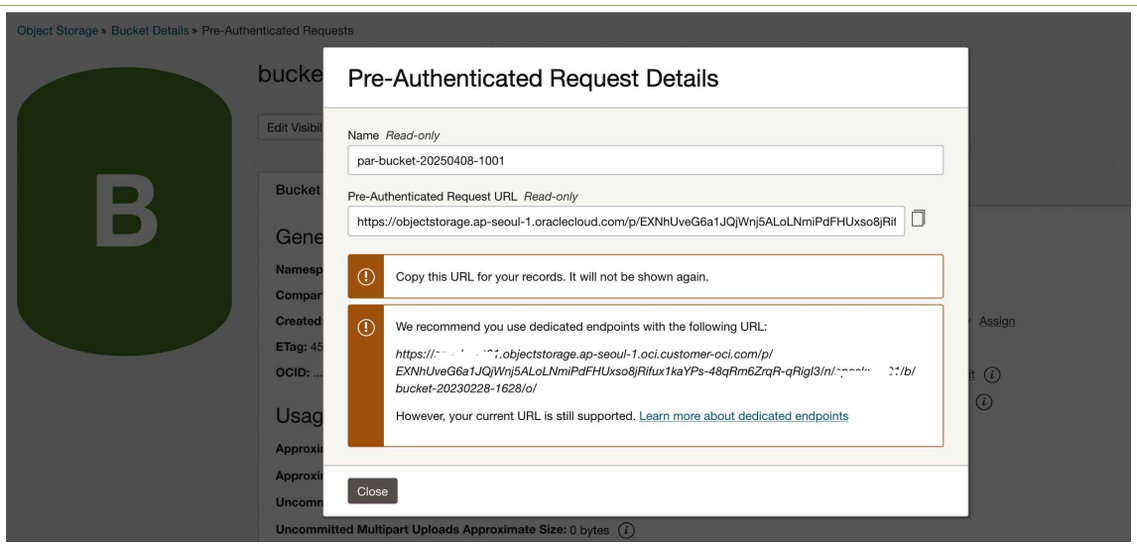
- 서명된 URL(Pre-authenticate Request) 생성 및 기본 설정
- 생성된 버킷 중 URL로 접근 시 통제 방안 적용이 필요한 리소스 선택



- OCI Object Storage에서 서명된 URL은 특정 객체 또는 버킷에 대한 제한된 시간 동안의 접근을 허용하는 URL로 버킷, 오브젝트 등 Target을 선택하고, 접근 권한(읽기, 쓰기, 읽기/쓰기)과 만료 시간을 설정할 수 있음



- 버킷/오브젝트 스토리지, 접근권한, 만료 시간이 설정 후 생성된 URL



4 참고 사항

- 버킷 스토리지: https://www.oracle.com/kr/cloud/storage/object-storage/
- 보안 모니터링: https://www.oracle.com/kr/security/cloud-security/cloud-guard/

1 기준

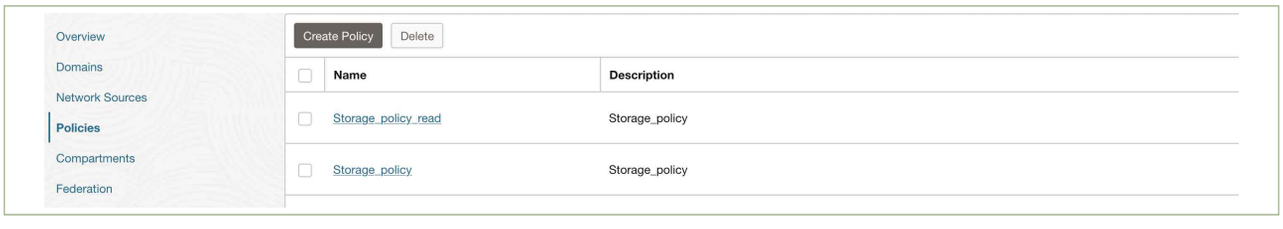
식별번호	기준	내용
7.2	**스토리지 권한 관리**	스토리지 목적에 따라 읽기, 쓰기 등의 권한을 관리하여야 한다.

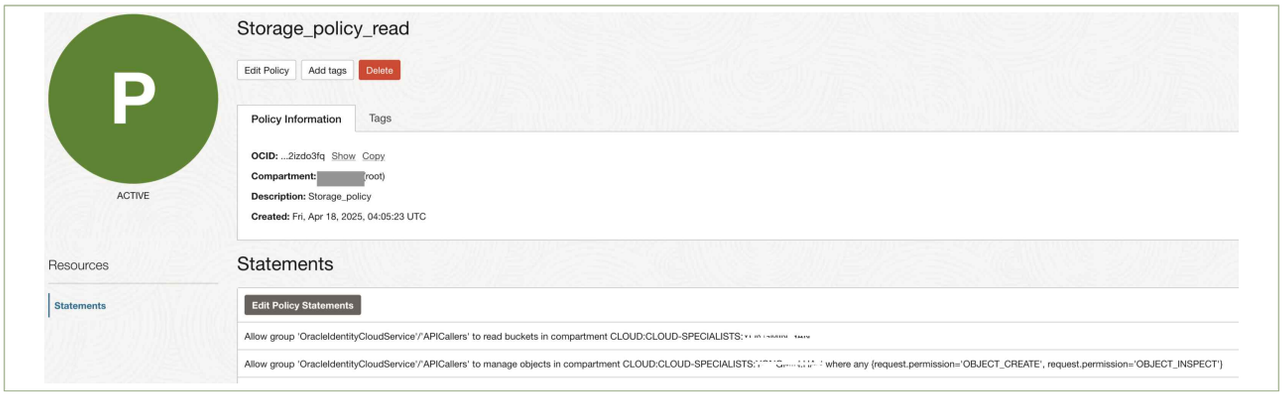
2 설명

- 스토리지 목적에 따라 읽기, 쓰기 등의 권한을 세분화하여 적용하여야 한다.
  1) 스토리지 객체에 관한 권한(읽기, 쓰기 등)을 세분화하여 목적에 따라 적용하여야 한다.
     5.1(2) 절차와 동일
  2) 스토리지 권한 부여 현황에 대한 모니터링 및 주기적 검토 수행

3 우수 사례

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' 에서 스토리지 접근권한을 수동으로 확인할 수 있으며 주기적으로 기존 생성한 접근권한을 모니터링 해야 함
  1) 스토리지 권한 부여 현황에 대한 모니터링 및 주기적 검토 수행
     - 기존에 생성한 스토리지 권한 리스트





1 기준

식별번호	기준	내용
7.3	**스토리지 업로드 파일 제한**	스토리지 목적에 따른 확장자 파일만 업로드 될 수 있도록 업로드 가능 파일을 제한하여야 한다.

2 설명

- 스토리지 목적에 따른 확장자 파일만 업로드 될 수 있도록 업로드 기능 파일을 제한하여야 한다.
  1) 스토리지 버킷 정책 설정을 통한 업로드 파일 확장자 제한 등
  2) 금융회사에서 스토리지 내 파일 업로드 시 확장자 등을 검증할 수 있는 절차 마련

3 우수 사례

- N/A

8. 백업 및 이중화 관리

8.1. 클라우드 이용에 관한 행위 추적성 증적(로그 등) 백업
8.2. 행위 추적성 증적 (로그 등) 백업 파일 무결성 검증
8.3. 금융회사 전산자료 백업
8.4. 금융회사 전산자료 백업 파일 무결성 검증
8.5. 행위 추적성 증적 전산자료 등 백업에 관한 기록 및 관리
8.6. 백업파일 원격 안전지역 보관
8.7. 주요 전산장비 이중화

8 백업 및 이중화 관리

1 기준

식별번호	기준	내용
8.1	**클라우드 이용에 관한 행위 추적성 증적(로그 등) 백업**	금융회사가 클라우드 이용 시 발생하는 다양한 행위 추적성 증적(가상자원, API, 네트워크서비스, 스토리지 관리, 계정 및 권한관리 등)의 보관기관 확보 등을 위해 백업을 수행(1년 이상 보관)하여야 한다.

2 설명

- 클라우드 이용 시 발생하는 로그에 대해 백업을 수행(1년 이상 보관) 하여야 한다.
  1) 스토리지 서비스를 별도로 생성 및 연동하여 행위 감사 로그 백업
  2) 클라우드 웹 콘솔 내 행위 감사 로그를 별도의 파일 형태로 다운로드 하여 별도로 보관

3 우수 사례

1) 스토리지 서비스를 별도로 생성 및 연동하여 행위 감사 로그 백업

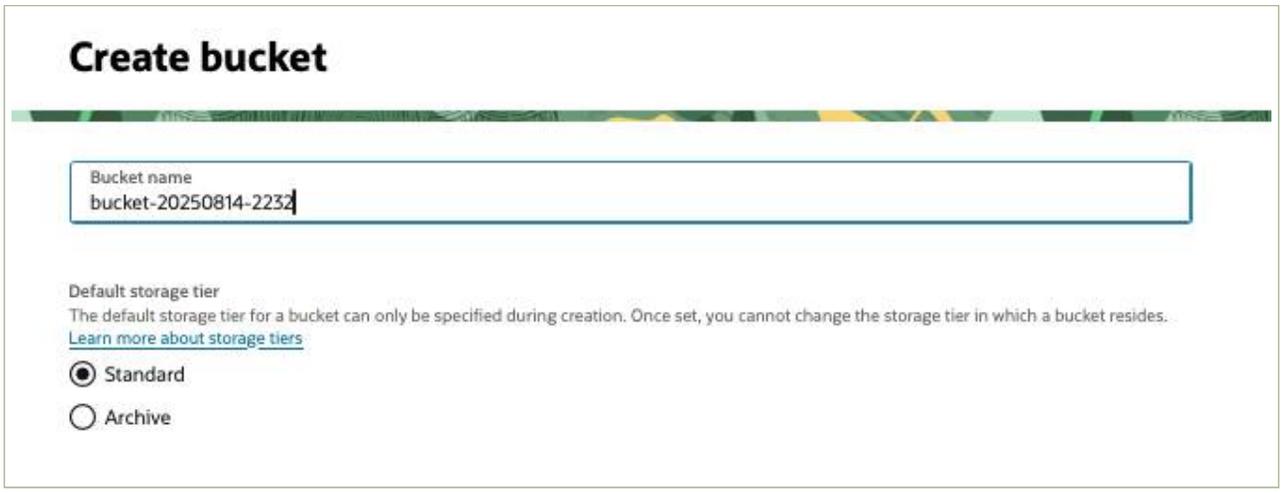
Oracle Cloud Infrastructure(OCI)에서 발생하는 행위 감사 로그의 보관기간은 365일이며, 1년 이상 보관해야 하는 규제 및 보안 요구사항을 충족하기 위해, OCI의 Logging, Service Connector hub, Object Storage 서비스를 연동하여 자동화된 백업 체계를 구축하여 OCI 내에서 로그의 장기 보관이 가능

(1) 구성 방법

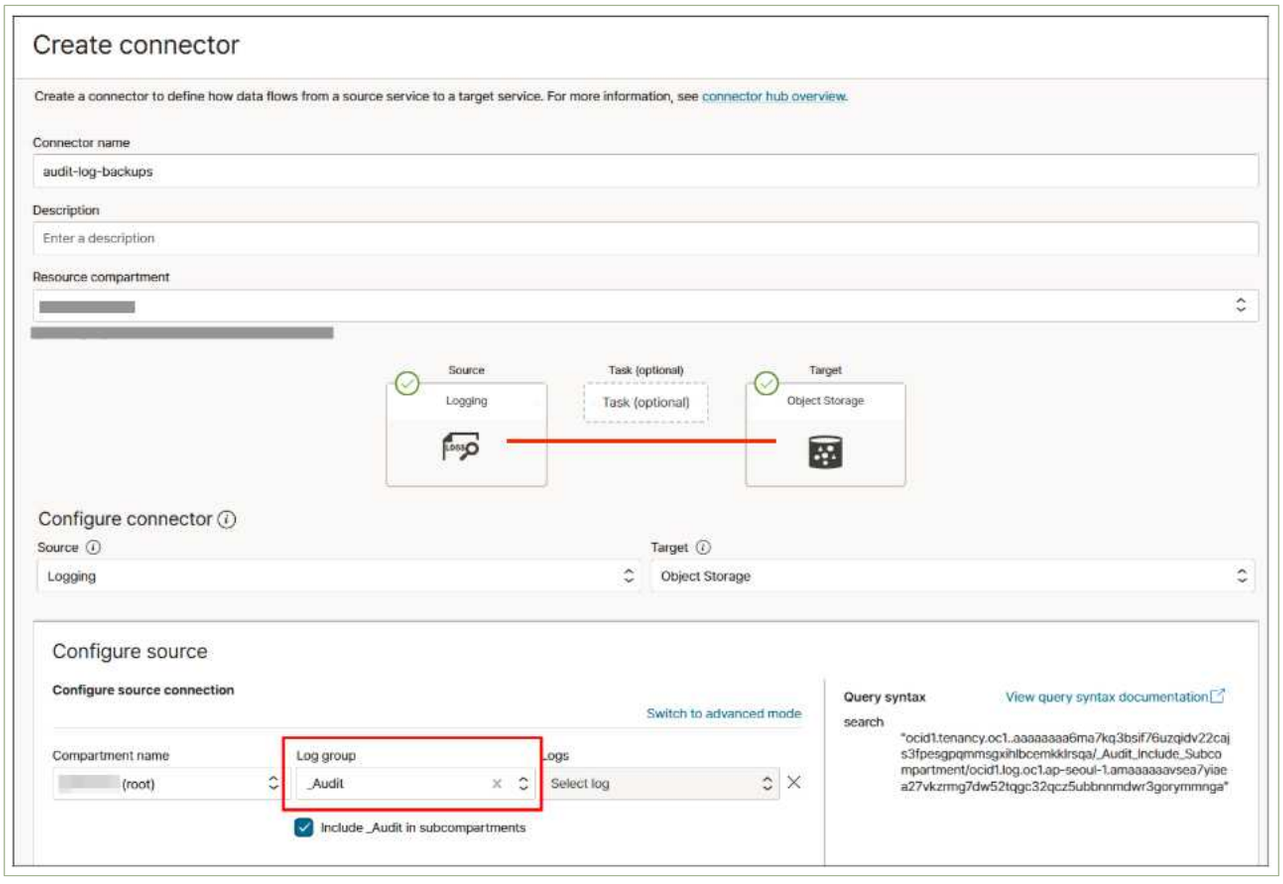
- 1단계: 로그를 저장할 오브젝트 스토리지 버킷 생성

  OCI 콘솔에서 스토리지(Storage) → 버킷(Buckets)으로 이동

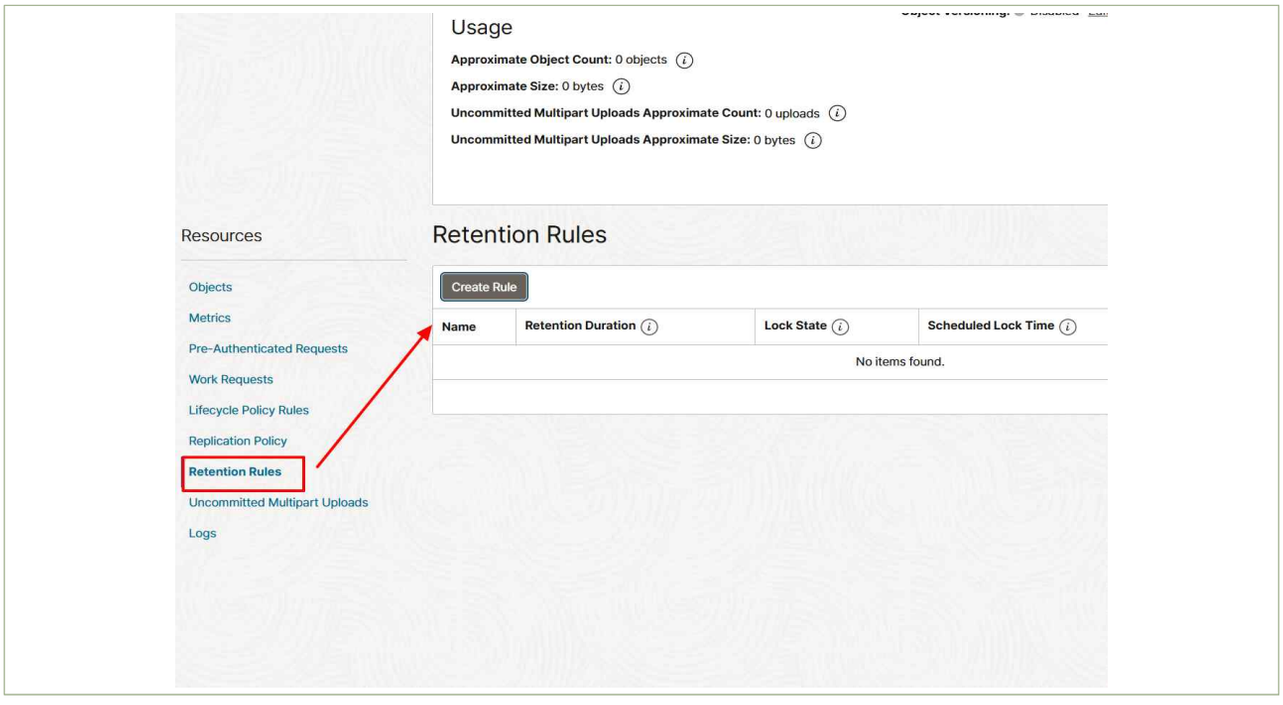
- 백업된 로그 파일을 저장할 버킷을 Object Storage로 생성

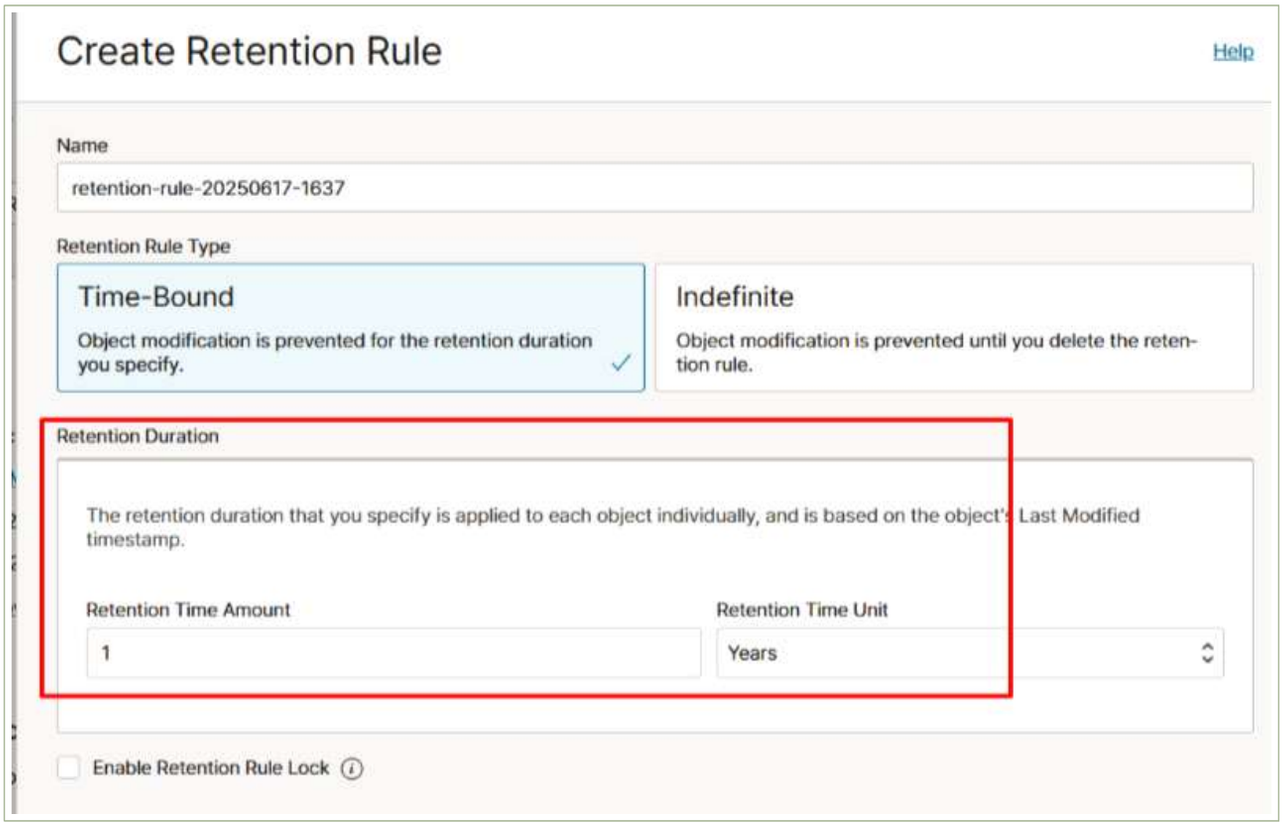


- 2단계: 로깅 서비스에서 감사 로그 활성화 확인
  - (Default 활성화) 테넌시의 루트 컴파트먼트에 대한 감사 로그는 활성화되어, _Audit이라는 이름의 로그가 자동으로 생성되어 있음
- 3단계: 서비스 커넥터 허브를 사용하여 로그 전송 설정
  - (OCI 콘솔) '홈' → Observability & Management → 서비스 커넥터(Service Connectors)으로 이동
  - 연동하고자 하는 Source는 로깅을 선택하고, Target은 Object Storage를 선택
  - Source: _Audit 로그를 선택하여 모든 감사 로그를 대상으로 지정 (하위 _Audit 컴파트먼트 포함)
  - Target: 1단계에서 생성한 버킷을 선택



- 4단계: 오브젝트 스토리지 보존 규칙 설정
  - 1년 이상의 보관 요구사항을 충족하도록 강제하고 실수로 인한 데이터 삭제를 방지하기 위해 Object Storage 버킷에 보존 규칙(Retention Rule) 설정 권고
  - 기간을 1년(Years) 이상으로 설정하고 규칙을 생성


Usage
Approximate Object Count: 0 objects
Approximate Size: 0 bytes
Uncommitted Multipart Uploads Approximate Count: 0 uploads
Uncommitted Multipart Uploads Approximate Size: 0 bytes
Resources
Objects
Metrics
Pre-Authenticated Requests
Work Requests
Lifecycle Policy Rules
Replication Policy
Retention Rules
Uncommitted Multipart Uploads
Logs
Retention Rules
Create Rule
Name
Retention Duration
Lock State
Scheduled Lock Time
No items found.

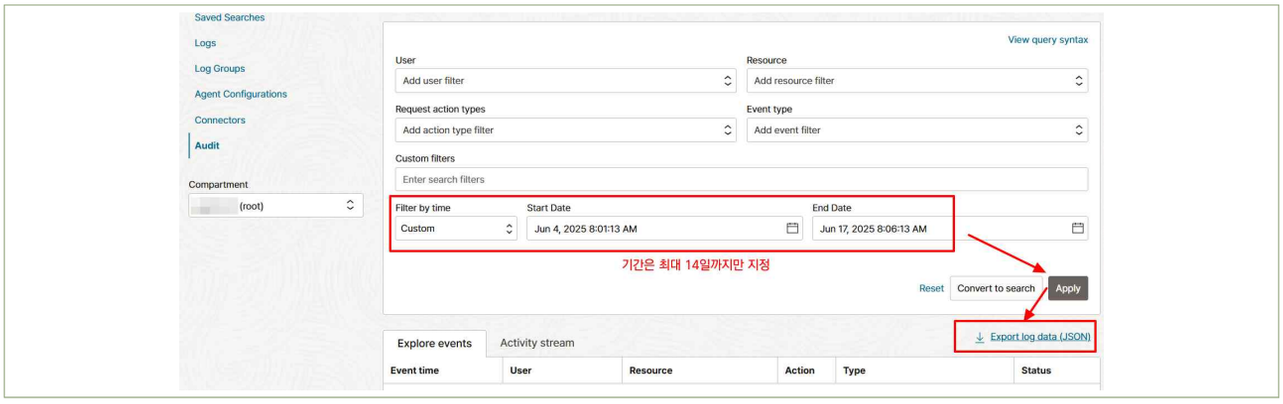

Create Retention Rule
Help
Name
retention-rule-20250617-1637
Retention Rule Type
Time-Bound
Object modification is prevented for the retention duration you specify.
Indefinite
Object modification is prevented until you delete the retention rule.
Retention Duration
The retention duration that you specify is applied to each object individually, and is based on the object's Last Modified timestamp.
Retention Time Amount
1
Retention Time Unit
Years
Enable Retention Rule Lock

2) 클라우드 웹 콘솔 내 행위 감사 로그를 별도의 파일 형태로 내려받아 별도로 보관

OCI는 콘솔에서 조회하는 서비스 및 기간에 따라 직접 감사 로그를 내려받는 몇 가지 방법을 제공함

• OCI 콘솔 감사(Audit) 서비스에서 직접 다운로드 (JSON)

(OCI 콘솔) '홈' → 'Observability & Management' → 감사(Audit)로 이동

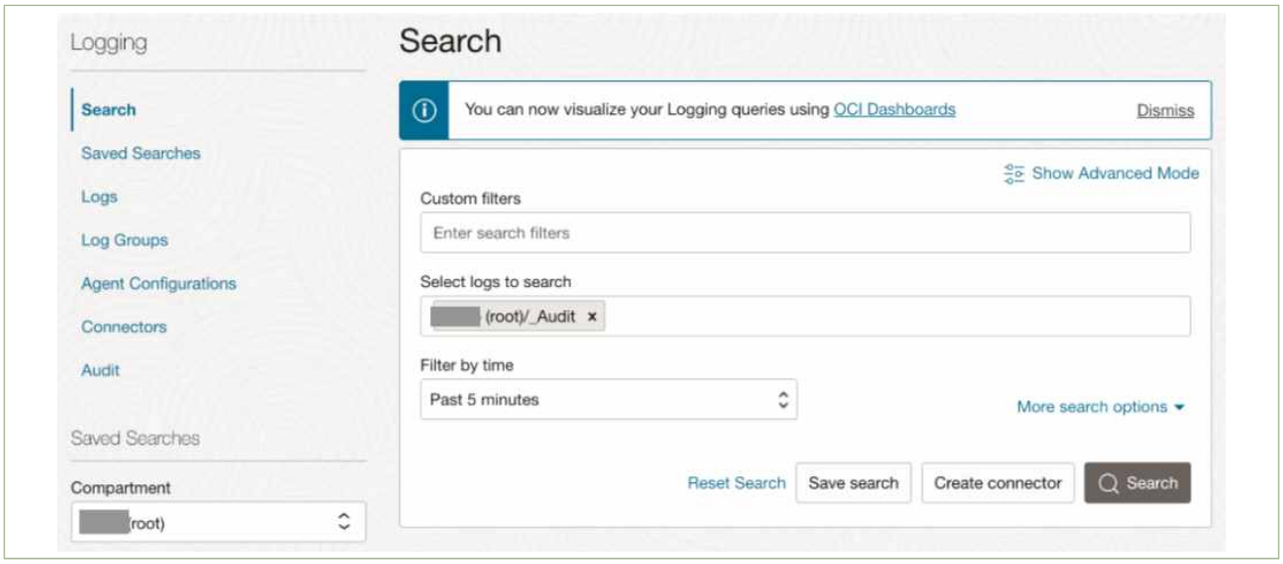


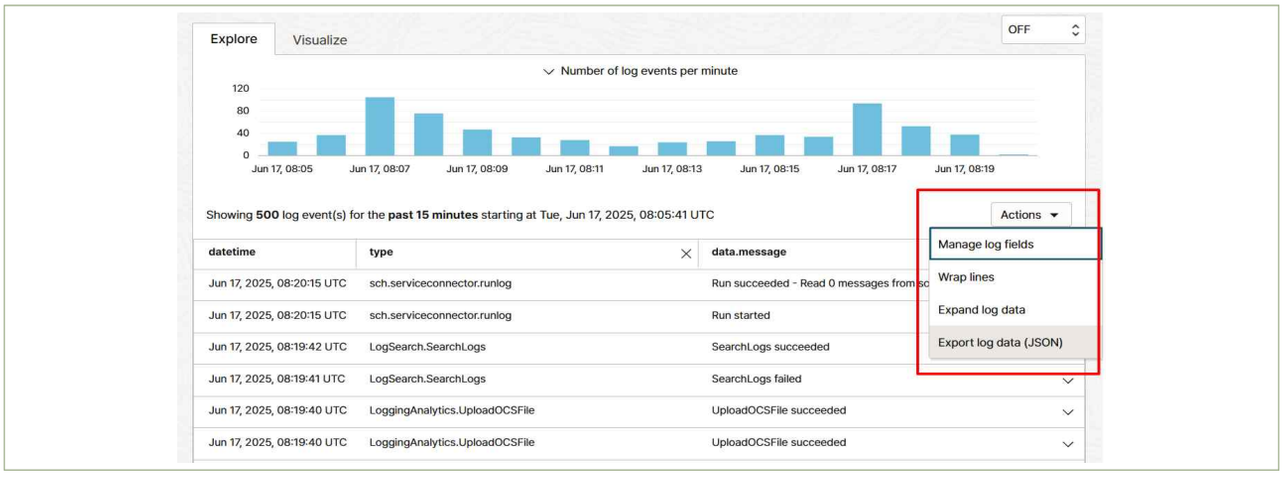
- 1회 조회 시 최대 14일, 최대 500건의 로그 이벤트 조회할 수 있으며, 이 단위로 다운로드 가능
- 그 이상의 건수를 조회하려면 CLI 또는 SDK/API를 사용

• OCI 콘솔 로깅(Logging) 서비스에서 다운로드 (장기, JSON)

(OCI 콘솔) '홈' → 'Observability & Management' → 로깅(OCI Logging) → 로그 탐색기(Log Explorer)로 이동

- 필터에서 원하는 조건을 선택하고 Search를 통해 로그를 조회
- 쿼리 실행 후, 결과 화면 우측 상단의 Action 드롭다운 메뉴를 클릭하고 내보내기(Export)를 선택

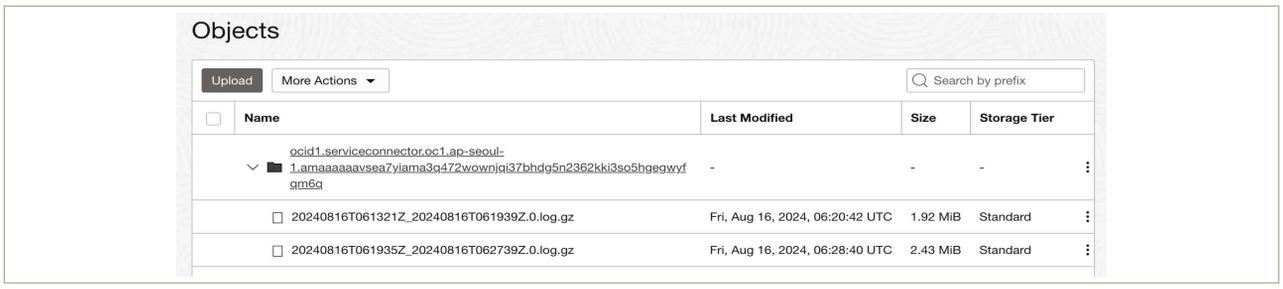




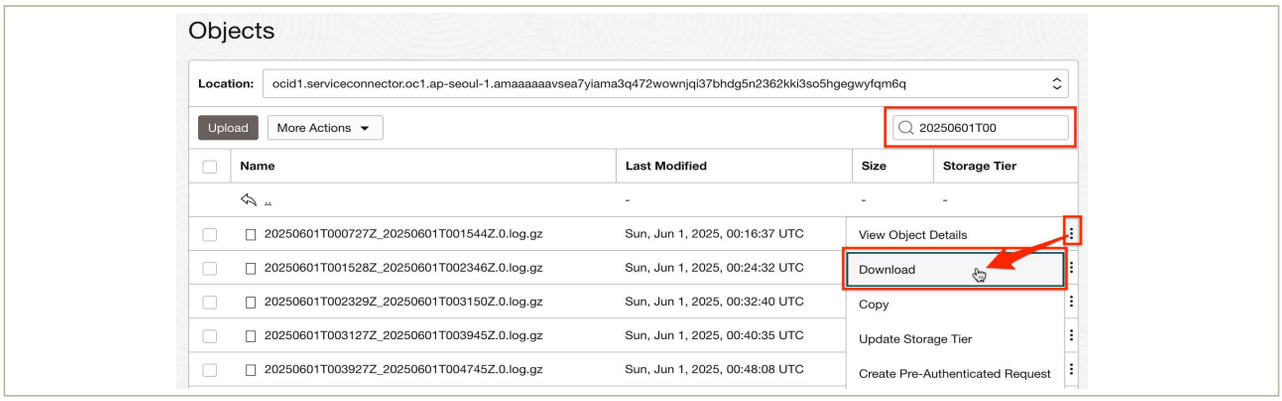
- 1회 조회 시 최대 14일, 최대 500건의 로그 이벤트 조회할 수 있으며, 이 단위로 다운로드 가능
- 그 이상의 건수를 조회하려면 CLI 또는 SDK/API를 사용

• Object Storage 백업에서 파일 형태로 다운로드하여 보관하기

- 앞선 단계에서 Connectors Hub를 통해 별도의 Object Storage로 백업 수행



- 파일명에 백업 날짜 및 수행 시간 정보가 있으므로, Object의 prefix에 원하는 날짜 시간대를 입력하여, 검색 후 다운로드
- 개별 단위로 하나씩 다운로드 가능
- 여러 파일을 일괄적으로 다운로드 받기 위해서는 CLI, SDK 등을 사용



1 기준

식별번호	기준	내용
8.2	**행위 추적성 증적(로그 등) 백업 파일 무결성 검증**	백업을 통해 보관되고 있는 행위 추적성 파일에 대한 무결성이 보장되어야 한다.

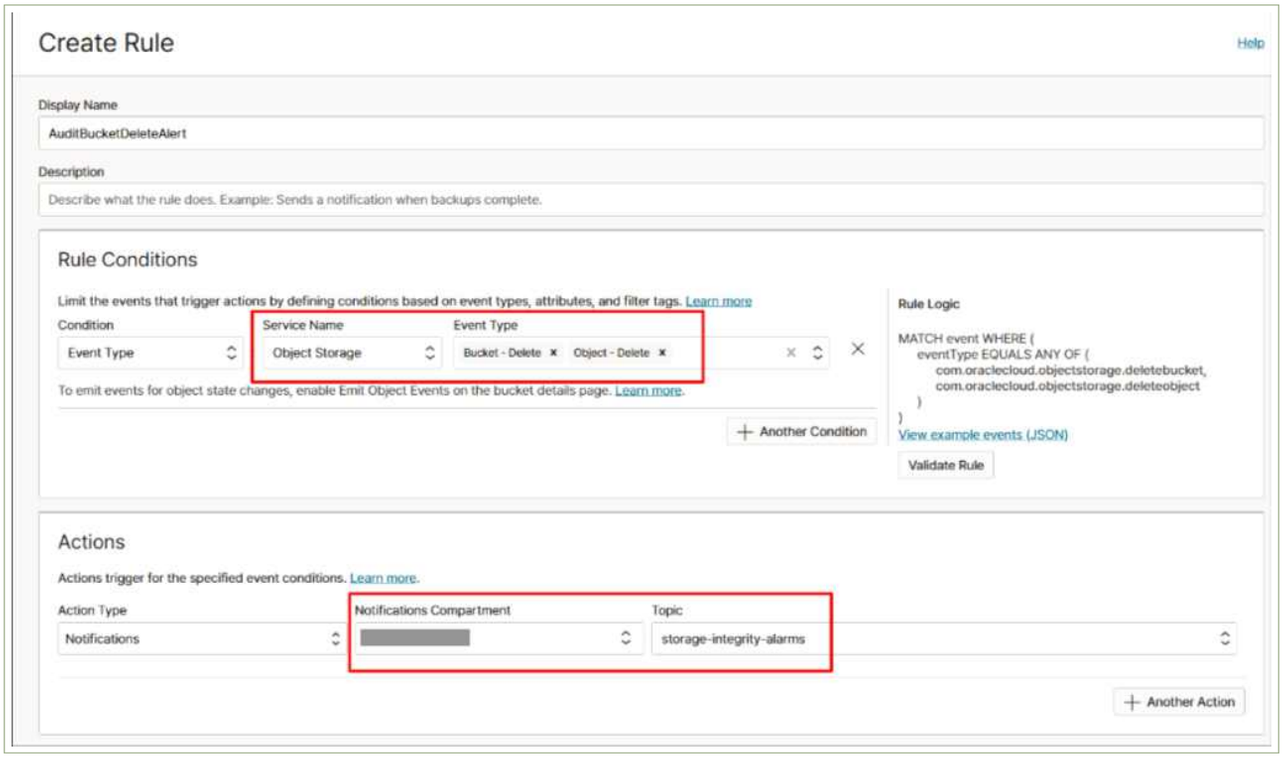
2 설명

- 이용자의 행위 추적성 백업 파일은 무결하게 보관하여야 한다.
  1) 클라우드 웹 콘솔 내 제공하는 행위 감사 로그 훼손 시 알람 등을 받을 수 있도록 설정
  2) 별도의 스토리지에 로그를 백업하여 행위 추적성 증적

3 우수 사례

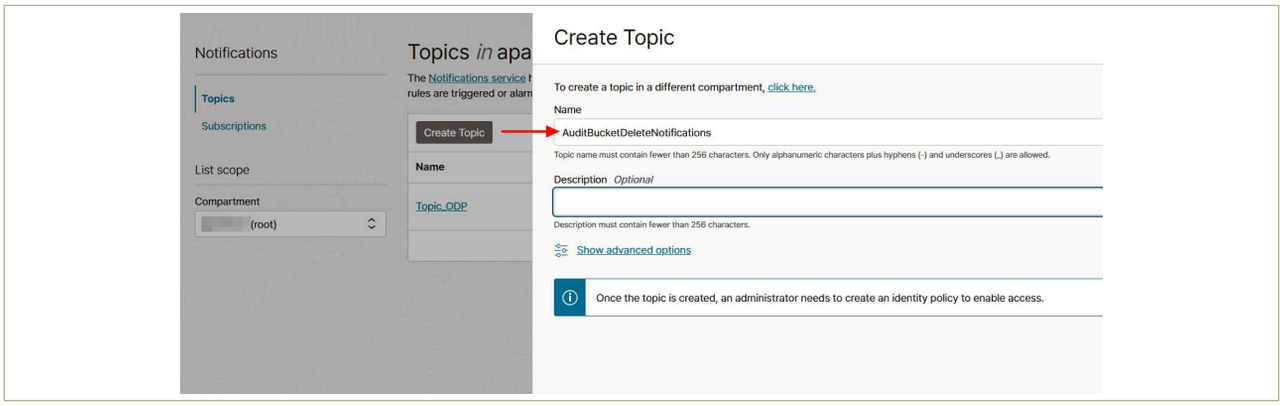
1) 클라우드 웹 콘솔 내 제공하는 행위 감사 로그 훼손 시 알람 등을 받을 수 있도록 설정
   오라클 클라우드 인프라스트럭처(OCI)에서는 기본적으로 Audit 서비스가 활성화되어 있으며, 모든 API 호출 및 사용자 작업(예: 리소스 생성, 수정 삭제 등) 자동 기록
   이 로그는 Audit Log에 저장되며, **기본적으로 무결성을 보장 설계**
   로그는 읽기 전용으로 저장되며, 사용자가 직접 수정하거나 삭제할 수 없음
2) 별도 스토리지 백업 기능을 통해 행위 추적성 증적
   (1) Service Connector Hub를 통해 별도의 Object Storage로 백업
   8.1.1 별도 스토리지 백업을 통해 감사 로그 백업 항목 참조
   (2) 별도의 스토리지로 이동한 감사 로그 백업의 보호를 위해 훼손 감지 및 알림 설정
   오라클 클라우드에서 감사 로그 자체는 시스템적으로 보호되지만, 로그가 저장된 Object Storage나 관련 리소스에 대한 무단 접근 또는 삭제 시도 감지 및 알림 수신 가능
   - Event Service를 사용한 삭제 작업 감지
     OCI의 Event Service를 사용하면 Object Storage 버킷에 대한 특정 이벤트(예: Delete Bucket, Delete Object) 감지 및 알림 트리거 설정
     특정 사용자의 작업을 필터링을 위해 이벤트 규칙 조건을 추가 가능
     - Event Rule 생성
       (OCI 콘솔) '홈' → 'Observability & Management' → 'Events'로 이동 Observability & Management → Events로 이동합니다.

- 규칙 생성
  - ‣ 규칙 이름을 지정(예: AuditBucketDeleteAlert)
  - ‣ 이벤트 유형(Event Type)
    - 서비스 이름: Object Storage
    - 이벤트 유형: Delete Bucket, Delete Object

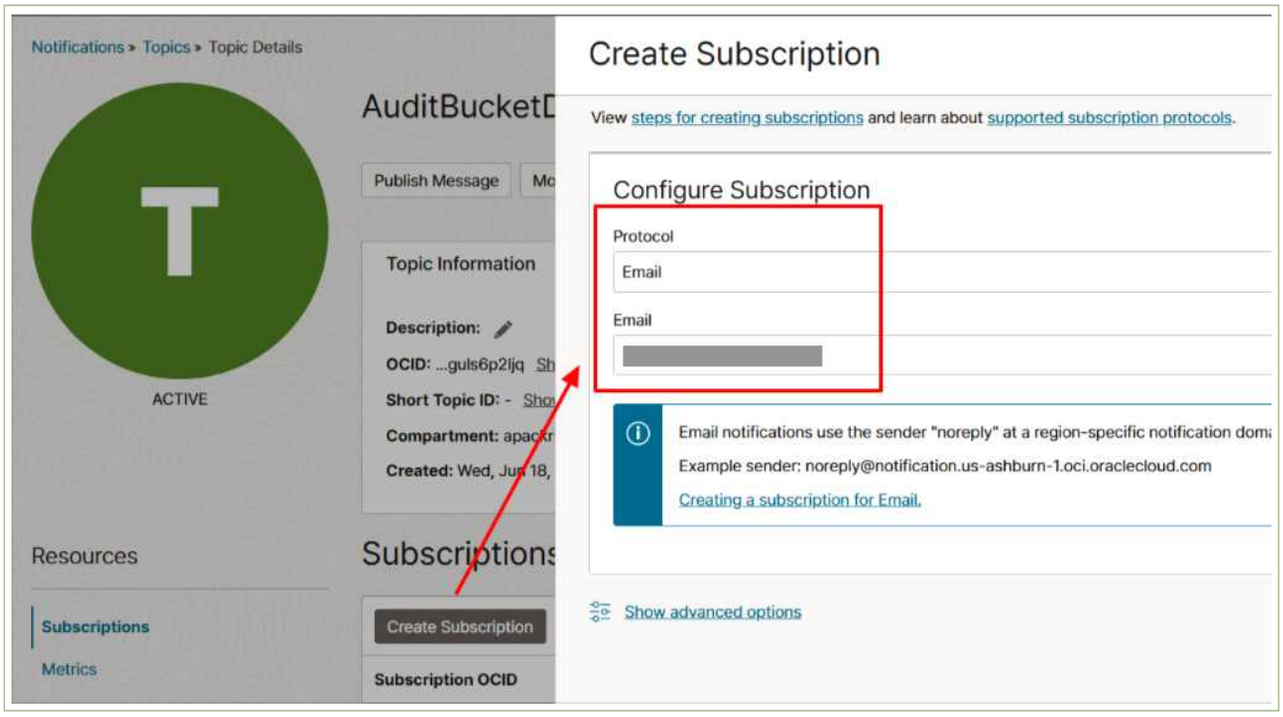


- Action
  - Action Type: Notification
  - Topic: 기존 알림 Topic을 선택하거나 새 Topic을 생성(예: Audit Bucket Delete Notifications)
- Notification 설정

  Notification Service를 설정하여 Event Service에서 감지된 이벤트를 알림으로 전송
  - Topic 생성: (OCI 콘솔) '홈' → 'Developer Service' → 'Application Integration' → 'Notification'으로 이동



- Event Rule과 연결: 버킷이 삭제될 경우, 위에서 생성한 Event Rule의 Action에서 생성한 Topic에 등록된 해당 이메일로 알림이 전송되도록 설정



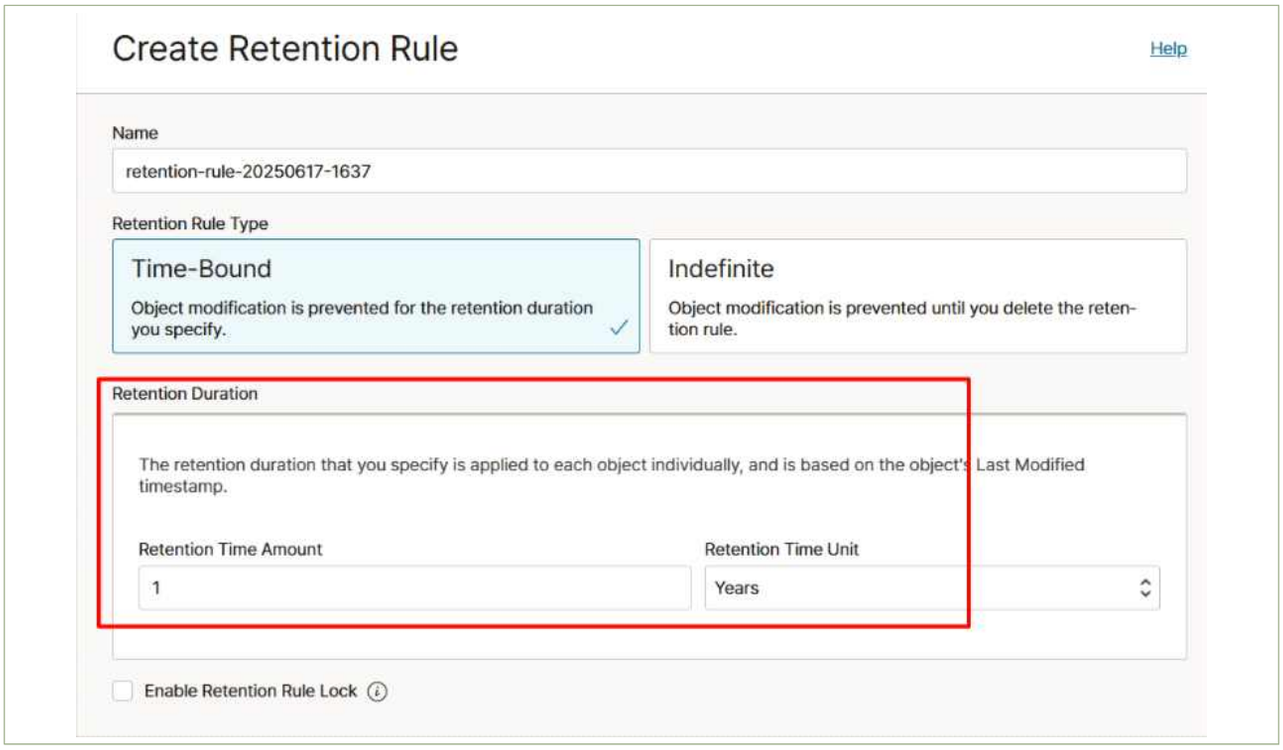
(3) Retention Rule 설정

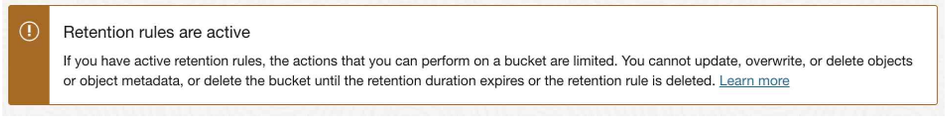
Retention Rule을 설정하면, OCI Object Storage 서비스 레벨에서 무단 삭제, 변경 시도를 막을 수 있으며, 별도의 알람 설정 등의 추가 작업이 필요 없음

▸ Retention Rule 설정

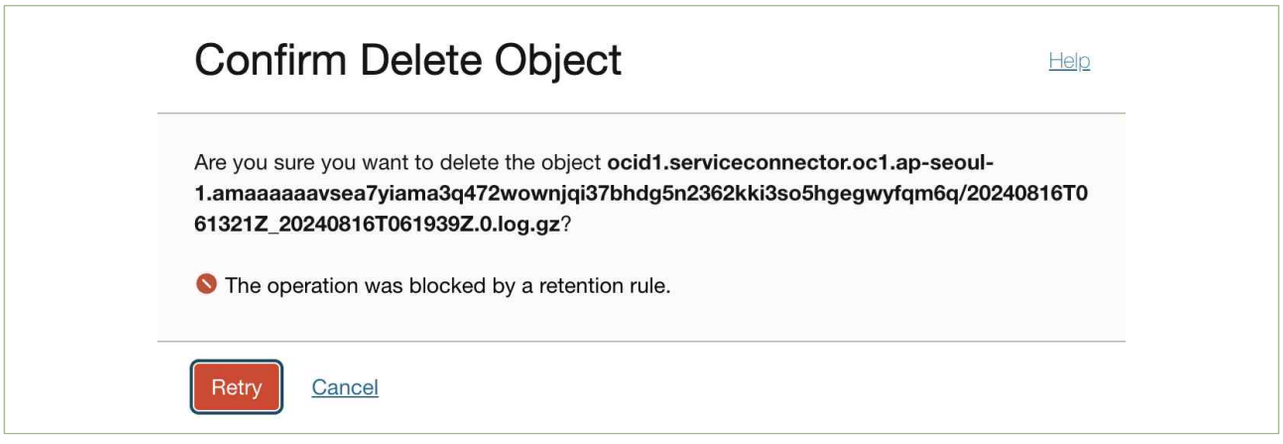
보존 규칙을 설정하면, 지정된 시간까지 변경 작업을 수행할 수 없으므로, 별도의 Object Storage에 백업된 로그도 무결성을 보장

- 규칙 유지를 위해 잠금 기능 제공





- Retention Rule에 따른 무결성 보장
  - Object에 대한 변경 또는 삭제 요청은 규칙에 따라 처리되지 않음



1 기준

식별번호	기준	내용
8.3	**금융회사 전산 자료 백업**	관련 법령(전자금융거래법, 전자금융감독규정 등)에 따라 백업이 필요한 금융회사 전산자료에 대해 백업을 수행하여야 한다.

2 설명

- 금융회사 클라우드 이용 시 관련 법령(전자금융거래법, 전자금융감독규정 등)에 따라 백업이 필요한 전산 자료에 대해서는 백업을 수행하여야 하며, 중요 업무인 경우 클라우드서비스와 관련한 중요 설정 파일 및 가상 시스템 이미지도 백업 대상에 포함하여야 한다. (중요도에 따라 1년 이상 보관)
  1) 클라우드 서비스 제공자가 제공하는 백업 서비스 이용
  2) 전산 자료를 별도로 다운 받아 금융회사가 관리하는 백업 서버 내 보관

3 우수 사례

1) 클라우드 서비스 제공자가 제공하는 백업 서비스 이용

(1) 오라클 클라우드 인프라스트럭처(OCI)의 백업 서비스와 금융 규제 준수 가능성

오라클 클라우드는 위에 언급된 규제 요건을 충족하기 위해 다양한 백업 및 복구 기능을 제공

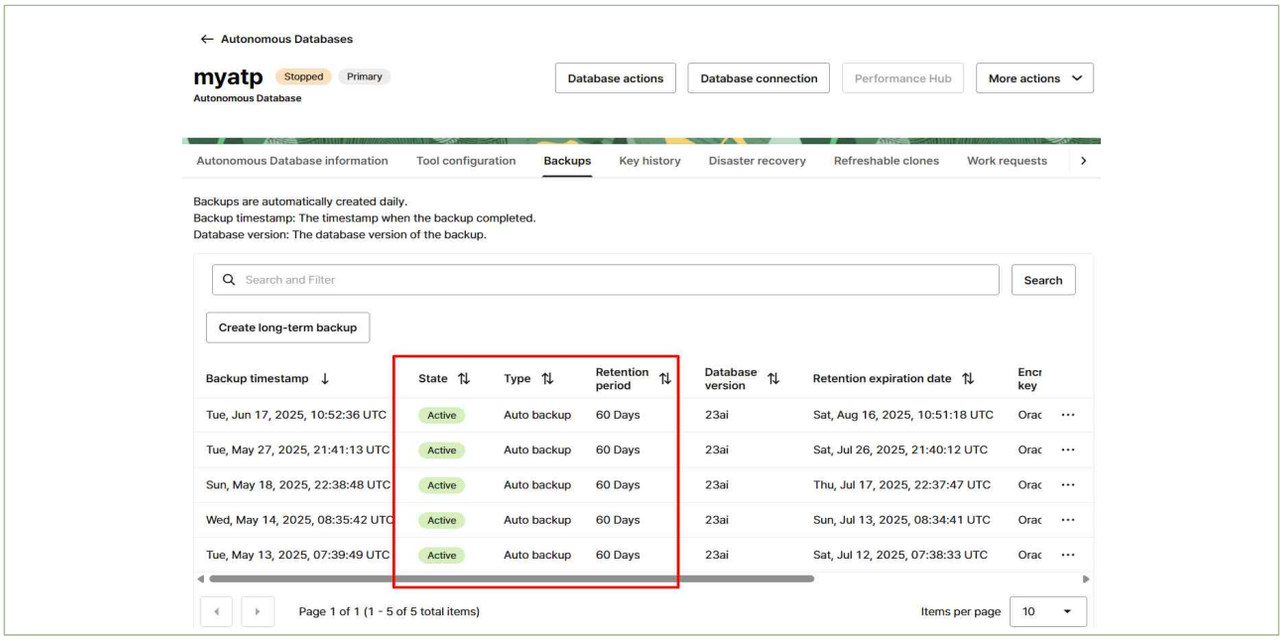
▸ 가상 시스템 이미지 및 중요 설정 파일 백업(Block Volume 및 Boot Volume 백업)

- Block Volume 백업
  - OCI는 컴퓨트 인스턴스에 연결된 블록 볼륨에 대한 백업 기능 제공
  - 전체 백업(Full Backup) 및 증분 백업(Incremental Backup): 두 가지 방식을 모두 지원하여 효율적인 백업 가능
  - 정책 기반 백업: 주간, 월간, 연간 등 미리 정의된 백업 정책을 블록 볼륨에 적용하여 자동화된 백업 수행. 예를 들어 “Gold Policy”는 일일, 주간, 월간, 연간 백업을 모두 포함하며 연간 백업은 5년까지 보존하여, “중요 설정 파일” 및 “가상 시스템 이미지” 백업 요구사항을 충족
  - Object Storage 저장: 모든 블록 볼륨 백업은 내부적으로 OCI Object Storage에 암호화되어 저장

- Boot Volume 백업: 시스템 전체 복구를 위한 “가상 시스템 이미지” 백업으로써, OS 및 시스템 설정이 포함된 Boot Volume도 블록 볼륨과 동일한 방식으로 백업 가능

• 데이터베이스 백업

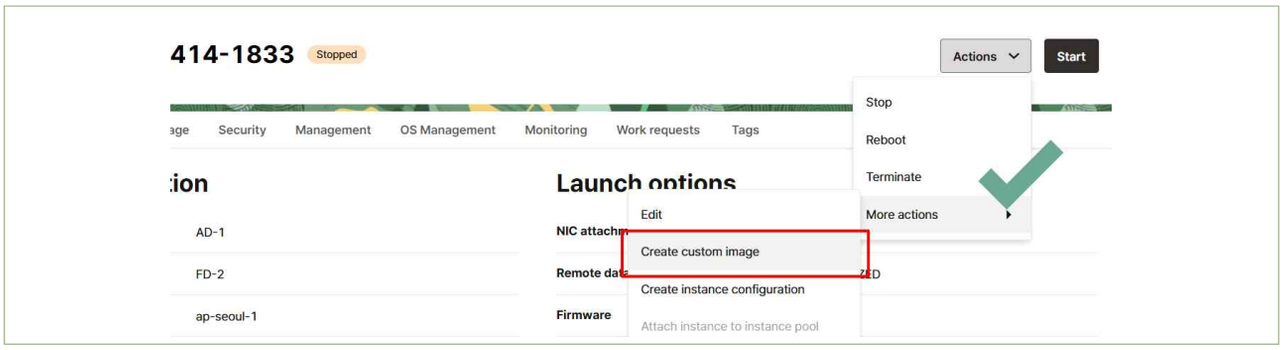
- OCI는 다양한 종류의 데이터베이스 서비스를 제공, 각 서비스는 자동 백업 기능을 제공
- OCI에서 제공하는 각 Database 서비스에 따라 상세 백업 기능 상이, 여기서는 대표적인 서비스인 OCI Autonomous Database를 기준으로 작성
- 증분 백업 및 전체 백업: 일반적으로 매일 증분 백업을 수행하고, 주 1회 전체 백업을 수행하도록 구성
- 보존 정책: 백업 보존 기간 설정 가능, Oracle Recovery Service를 통해 보호 정책을 사용하여 데이터베이스 백업 보존을 제어. 단, 금융 규정의 1년/5년 보존 요구사항을 충족하기 위해 장기 보존(Long-Term Retention) 정책을 별도로 설정하거나, 백업 데이터를 OCI Object Storage에 수동 또는 자동화된 스크립트로 복사하여 장기간 보관 필요
- PITR(Point-in-Time Recovery): 특정 시점으로 복구하는 기능을 제공하여 데이터 손실 최소화



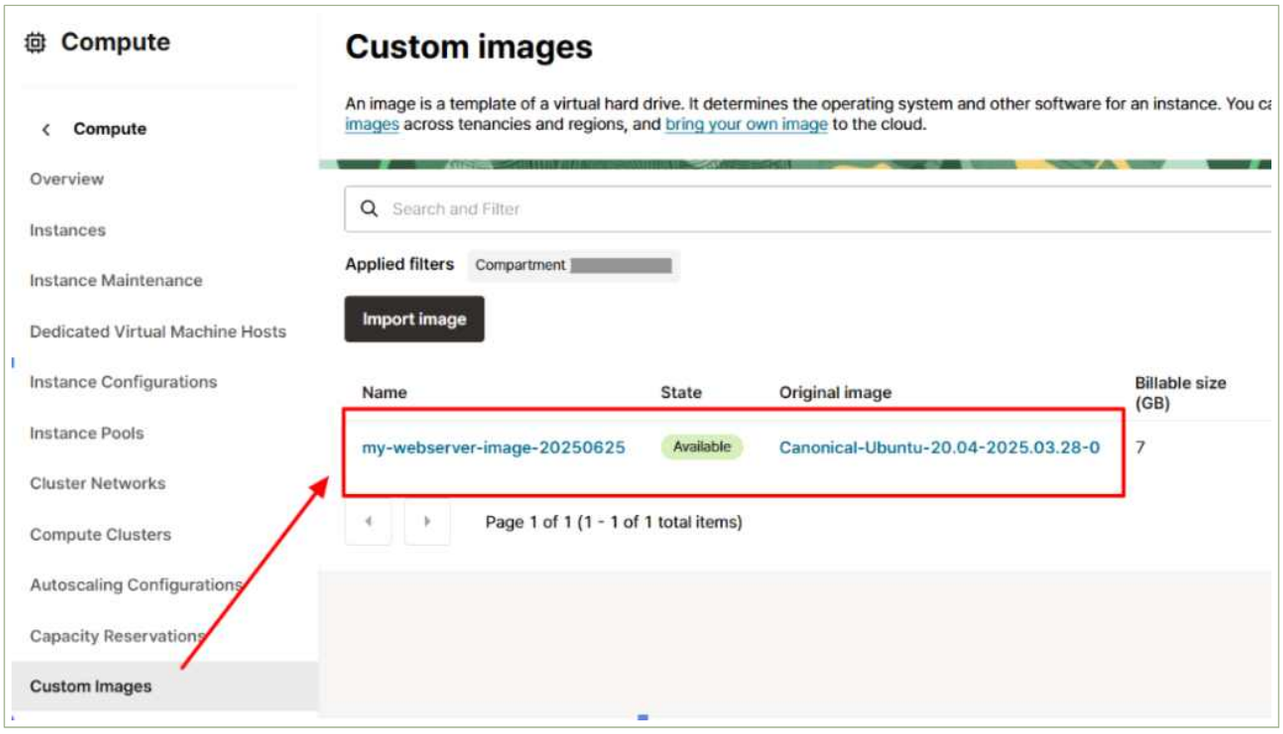
2) 전산 자료를 별도로 다운로드하여 금융회사가 관리하는 백업 서버 내 보관

(1) Custom Image

- (OCI 콘솔) '홈' → 'Compute' → 'Instance'로 이동 Compute → Instance로 이동합니다.
- 인스턴스를 선택한 후 오른쪽 우측 상단 드릴 다운 메뉴에서 사용자 정의 이미지 생성(Create custom image)를 클릭



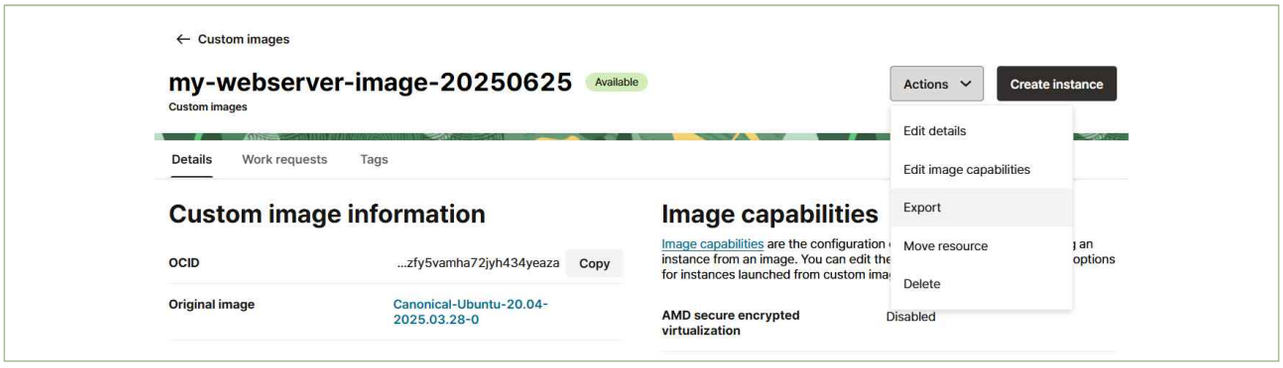
- 이미지 생성 작업은 몇 분 정도 소요되며, Work requests 또는 Compute → Custom Images 메뉴에서 진행 상황을 확인 가능



• Custom Image Export 및 오브젝트 스토리지로 이동

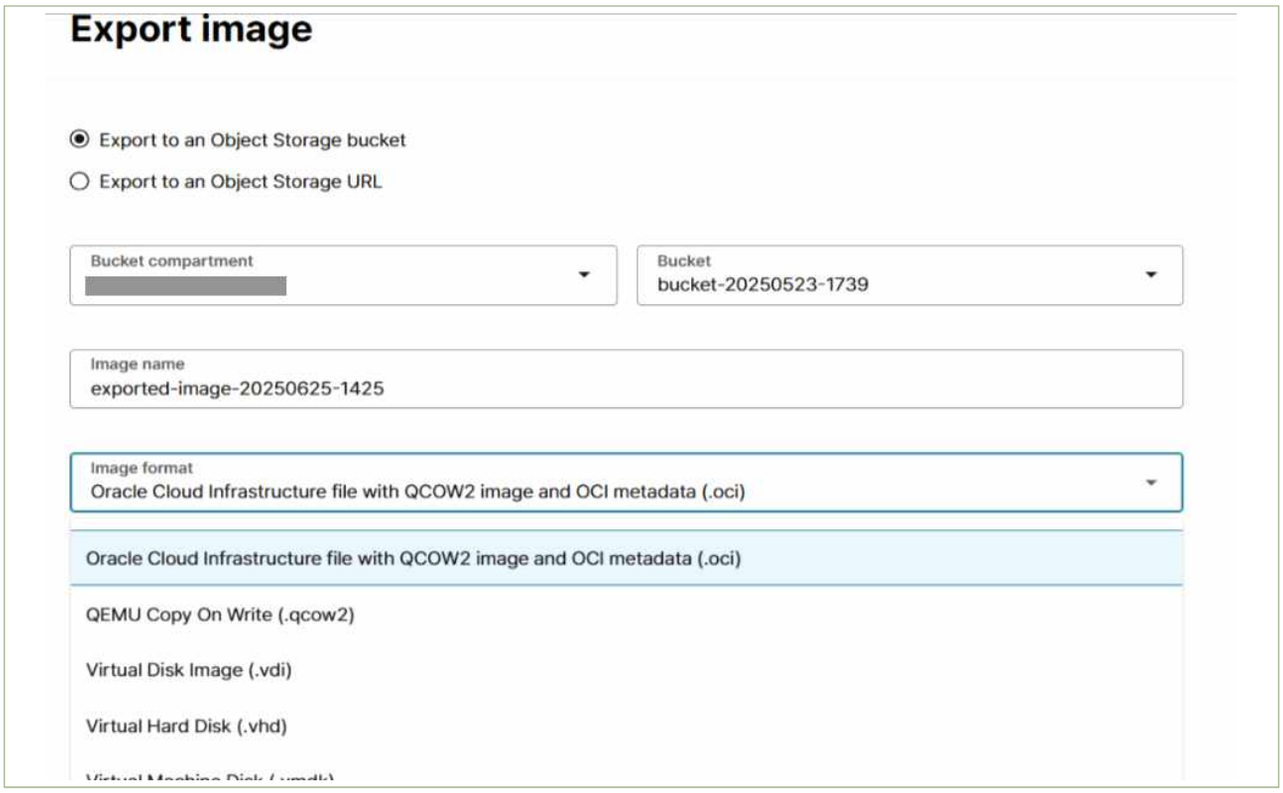
(OCI 콘솔) '홈' → 'Compute' → 조금 전 생성한 Available 상태가 된 커스텀 이미지를 클릭한 후 이미지 세부 정보 페이지 상단의 내보내기(Export) 버튼 클릭

Compute → 조금 전 생성한 Available 상태가 된 커스텀 이미지를 클릭한 후 이미지 세부 정보 페이지 상단의 내보내기(Export) 버튼 클릭



- 다음으로 내보내기: Object Storage Bucket
- 버킷: 이미지를 저장할 오브젝트 스토리지 버킷을 드롭 다운 목록에서 선택
- 객체 이름: 버킷에 저장될 파일의 이름을 입력
- 이미지 형식: 내보낼 이미지의 파일 형식을 선택
- 이미지 내보내기 창에서 다음을 설정

- OCI: QCOW2 이미지와 OCI 메타데이터를 포함한 형식, 다른 OCI 테넌시나 리전으로 가져올 때 권장
- QCOW2: KVM 등에서 널리 사용되는 가상 디스크 형식
- VMDK: Vmware 환경에서 사용되는 형식
- VHD: Hyper-V 환경에서 사용되는 형식



(2) Block Storage

- OCI에서 제공하는 Block Storage 서비스의 백업 기능으로 백업한 파일은 사용자가 직접 내려받을 수 없음
- 대안으로 별도의 툴을 사용해 먼저 OCI Object Storage에 백업하고, 다시 자체 데이터센터로 이동
- "8.6 백업 파일 원격 안전지역 보관 〉 2) 금융회사 자체 데이터센터로 소산하여 보관"과 동일한 과정으로, 자세한 절차는 해당 항목을 참조

(3) Database

- Autonomous Database에서 관리형 서비스 제공하는 자동 백업에 대해 사용자가 직접 다운로드 하는 기능은 제공하지 않음
- 자체 데이터센터로 백업을 원하는 경우, Data Pump를 통해 OCI Object Storage에 백업하고, 다시 자체 데이터센터로 이동

- "8.6 백업 파일 원격 안전지역 보관 〉 2) 금융회사 자체 데이터센터로 소산하여 보관"과 동일한 과정으로, 자세한 절차는 해당 항목을 참조

(4) Object Storage

- 자체 데이터센터에서 OCI 환경으로 접근이 가능한 위치에서 아래 설정을 통해 Object Storage Sync 기능을 사용하여 백업을 다운로드
- "8.6 백업 파일 원격 안전지역 보관 〉 2) 금융회사 자체 데이터센터로 소산 하여 보관"과 동일한 과정으로, 자세한 절차는 해당 항목을 참조

4 참고 사항

- Data Integrity (Object Storage의 데이터 무결성):
  https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm#Data_Integrity
- Server-Side Encryption (저장 데이터 암호화):
  https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/encryption.htm

1 기준

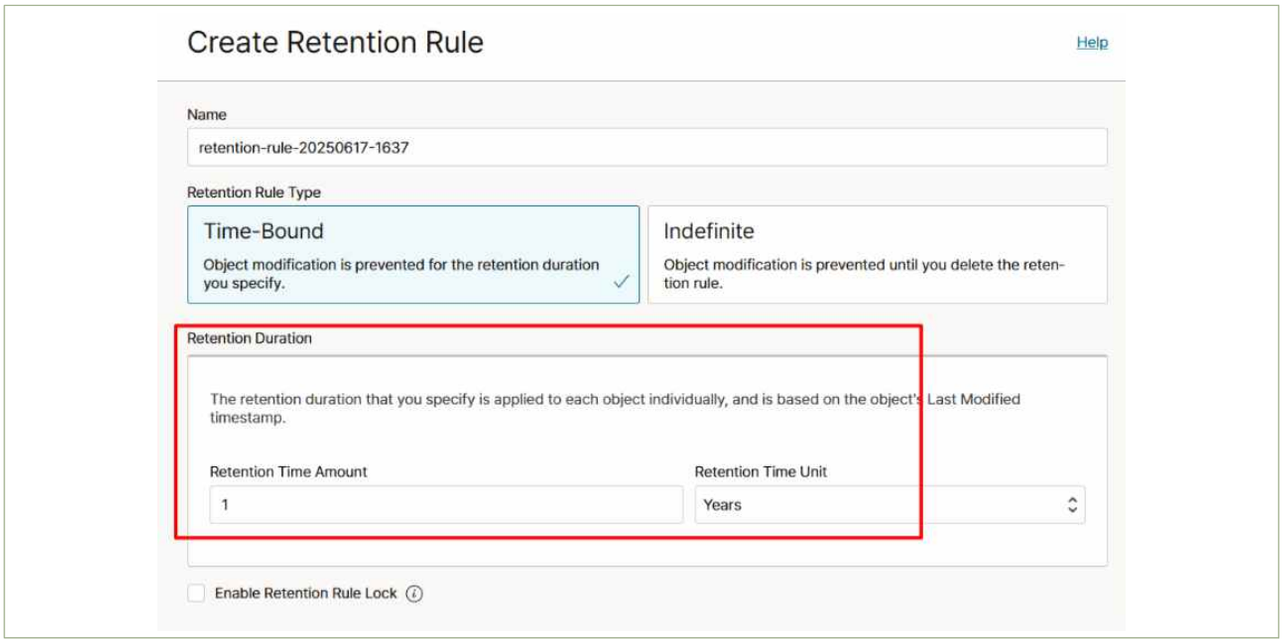
식별번호	기준	내용
8.4	**금융회사 전산 자료 백업 파일 무결성 검증**	백업을 통해 보관되고 있는 전산 자료에 대한 무결성이 보장되어야 한다.

2 설명

- 금융회사의 전산 자료 백업 파일은 무결하게 보관하여야 한다.
  1) 클라우드 서비스 제공자가 제공하는 스토리지로 백업하는 경우 스토리지 내 파일이 훼손될 시 알람을 받을 수 있도록 설정
  2) 금융회사가 운영하는 백업 서버로 백업하는 경우 무결하게 보관

3 우수 사례

1) 클라우드 서비스 제공자가 제공하는 스토리지로 백업하는 경우 스토리지 내 파일이 훼손될 시 알람을 받을 수 있도록 설정
   (1) Retention Rule 설정 (아랫줄 중복으로 삭제함)
   - 보존 규칙을 설정하면, 지정된 시간까지 변경 작업을 수행할 수 없게 되어, 별도의 Object Storage에 백업된 로그에 대해서도 무결성 보장
     - 규칙 유지를 위해 잠금을 하는 기능 제공



- Object에 대한 변경 또는 삭제 요청은 규칙에 따라 처리되지 않음

(2) 물리적 손상에 대한 자동 복구(내부 무결성)

OCI 오브젝트 스토리지는 데이터의 물리적 손상에 대해 별도의 설정 없이도 자동으로 무결성 검사 및 복구

- 높은 내구성: OCI 오브젝트 스토리지(Object Storage)는 99.999999999% (Eleven 9s)의 내구성을 보장하고, 여러 가용성 도메인과 장애 도메인에 데이터를 중복 저장
- 자동 복구(Self-Healing): 저장된 모든 데이터에 대해 지속적으로 체크섬(Checksum)을 확인하여 데이터 무결성 모니터링
- 데이터 손상 감지 시, 시스템은 자동으로 중복 저장된 다른 사본을 이용하여 원본을 복구하고, 이 과정은 사용자에게 영향없이 투명하게 수행

- OCI Object Storage 내구성 및 복원 관련
  https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm
  https://www.oracle.com/cloud/storage/object-storage/faq/
  https://blogs.oracle.com/cloud-infrastructure/post/first-principles-redundancy-recovery-durability

2) 금융회사가 운영하는 백업 서버로 백업하는 경우 무결하게 보관

금융회사가 운영하는 백업 서버로 백업 파일을 옮기는 경우, 원복 백업의 무결성을 보장 및 전달 과정에서도 훼손 방지 필요. 데이터 변조나 손실 없이 원본 자료의 신뢰성을 유지하고, 규제 준수를 충족하기 위해 필요함

(1) 무결성 보장 메커니즘

- 원본 백업 데이터의 무결성(Source Integrity)

  전송을 시작하기 전, OCI에 있는 원본 백업 데이터 무결성 신뢰 확보 단계

  - 데이터 중복화 및 자가 복구(Redundancy & Self-Healing)
    - OCI의 블록 볼륨 및 부트 볼륨 서비스는 데이터를 여러 스토리지 서버와 Fault Domain에 걸쳐 중복으로 저장
    - OCI는 내부적으로 체크섬을 사용하여 저장된 데이터 블록의 무결성을 지속적으로 모니터링
    - 물리적 오류 등으로 데이터 손상(Bit Rot) 감지 시, 시스템은 자동으로 다른 복제본을 사용하여 원본을 복구
  - 전송 데이터 암호화(Encryption at Rest)
    - OCI의 모든 블록/부트 볼륨 백업 데이터는 기본적으로 AES-256 알고리즘으로 암호화되어 저장, 데이터 기밀성을 보장 및 변조 방지 추가 보호 계층 역할

- 데이터 전송 과정의 무결성(Integrity in Transit)

  백업 데이터가 OCI에서 금융사 백업 서버로 이동하는 동안 데이터가 변조 또는 손상 방지 단계

  - 암호화된 보안 전송 채널 구축
    - 권장 방법: OCI FastConnect를 사용하여, 인터넷을 경유하지 않는 전용 사설 회선을 구축, 중간자 공격(MIMT)를 차단하여 가장 안전하고 안정적인 전송 채널을 보장
    - VPN(Site-to-Site VPN) 사용: 인터넷을 통해 전송 시, 강력한 암호화 터널(IPSec)로 데이터 보호
  - 전송 데이터 검증을 위한 해시(Hash) 값 활용
    - 전송 중 무결성을 보장하는 가장 핵심 기술로, 디지털 지문을 통해 파일이 원본과 정확히 일치하는지를 검증(SHA-256)

4 참고 사항

- Using Retention Rules to Preserve Data:
  https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/usingretentionrules.htm
- Object Storage API – PutObject:
  https://docs.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/Object/PutObject
- Oracle Cloud for Financial Services:
  https://www.oracle.com/financial-services/cloud/

1 기준

식별번호	기준	내용
8.5	**행위추적성 증적 및 전산자료 등 백업에 관한 기록 및 관리**	행위추적성 증적 및 금융회사 전산자료 백업 시 백업내역을 기록하고 관리하여야 한다.

2 설명

- 행위 추적성 증적 및 전산 자료 등 백업 시 백업 내역을 기록하고 관리하여야 한다.
  1) 백업 대상, 백업 주기, 백업 담당자 등 정책 수립
  2) 주기적으로 백업 정상 여부에 대한 모니터링 및 검토

3 우수 사례

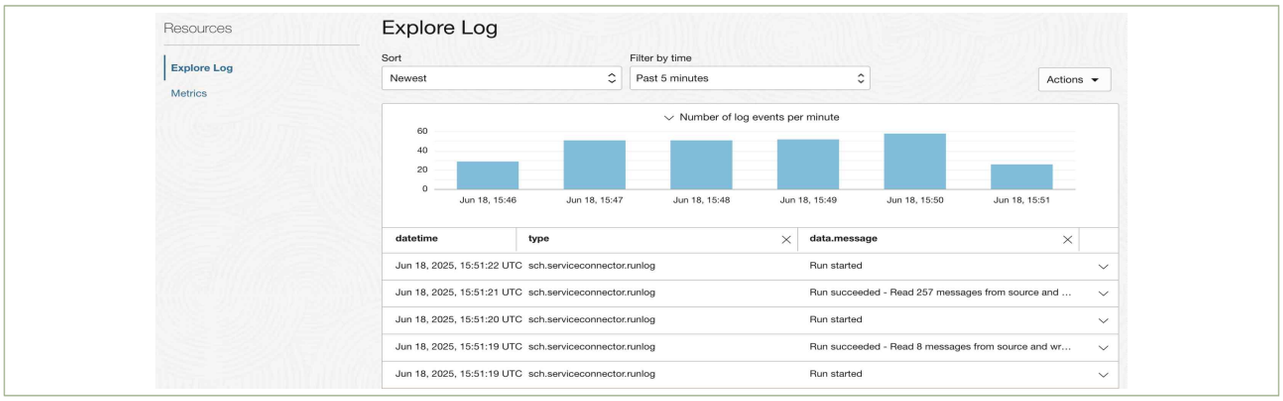
1) 백업 대상, 백업 주기, 백업담당자 등 정책 수립

백업 대상		백업 주기
행위 추적성 증적	Audit Log	OCI Audit Log는 기본 365일 동안 보관됨 백업은 OCI Connector Hub를 통해 지속적으로 Object Storage에 저장하는 방식으로 따로 백업 주기는 없음
전산 자료	Block Storage Backup (Boot / Block Volume)	Gold(연, 월, 주, 일), Silver(연, 월, 주), Bronze(연, 월) 백업 정책을 제공 필요하면, 사용자가 커스텀 백업 정책을 추가할 수 있음
	DB Backup	Autonomous Database 기준으로 매일 자동으로 백업됨

(1) Audit Log 백업

- 백업 주기
  - Audit Log 백업이 필요한 경우, 추가 Connector Hub를 활용하여, 대상지로 백업하도록 추가 구성하는 방법이며, Audit Log 서비스에서 제공하는 기능이 아니므로 별도 백업 주기 설정은 없음
  - Audit Log가 발생하면, OCI Connector Hub를 통해 지속적으로 Object Storage로 저장하기 때문에, 실행 주기를 따로 지정하지는 않음
  - (OCI 콘솔) '홈' → 'Observability & Management' → 'Logging' → 'Connectors'에서 앞서 생성한 Connector로 이동 → Connector의 로그로 이동
  - 실행 로그에서 거의 초 단위로 지속적으로 실행되는 것을 확인 가능 Observability & Management → Logging → Connectors에서 앞서 생성한 Connector로 이동합니다.

Connector의 로그로 이동. 실행 로그에서 거의 초 단위로 지속적으로 실행되는 것을 확인할 수 있음



- 백업 담당자 설정

  OCI IAM 정책에서 백업 담당자에게 백업에 필요한 권한(Audit 서비스, Connector Hub, Object Storage 등)을 부여

  - 정책 샘플 예시

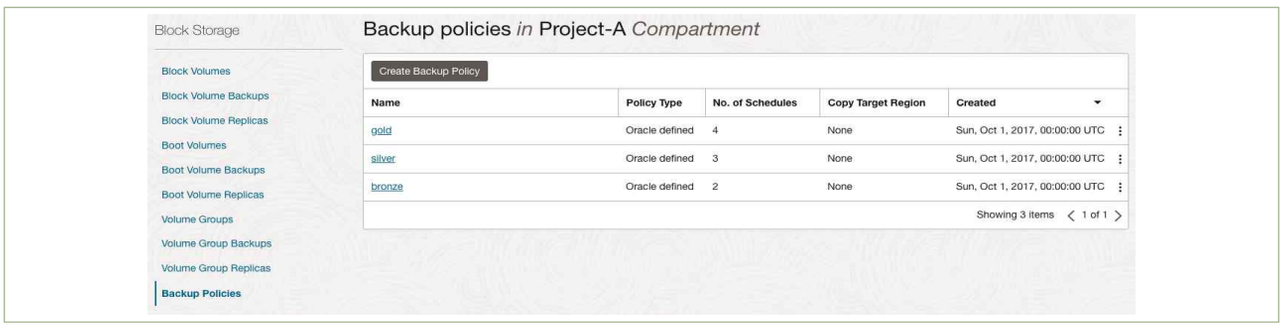
```
Allow group BackupAdmins to read audit-events in tenancy
Allow group BackupAdmins to manage serviceconnectors in compartment
<compartment-name>
Allow group BackupAdmins to manage object-family in compartment
<compartment-name> where target.bucket.name=/audit-log-*/
```

(2) Block Storage 백업

- 백업 주기

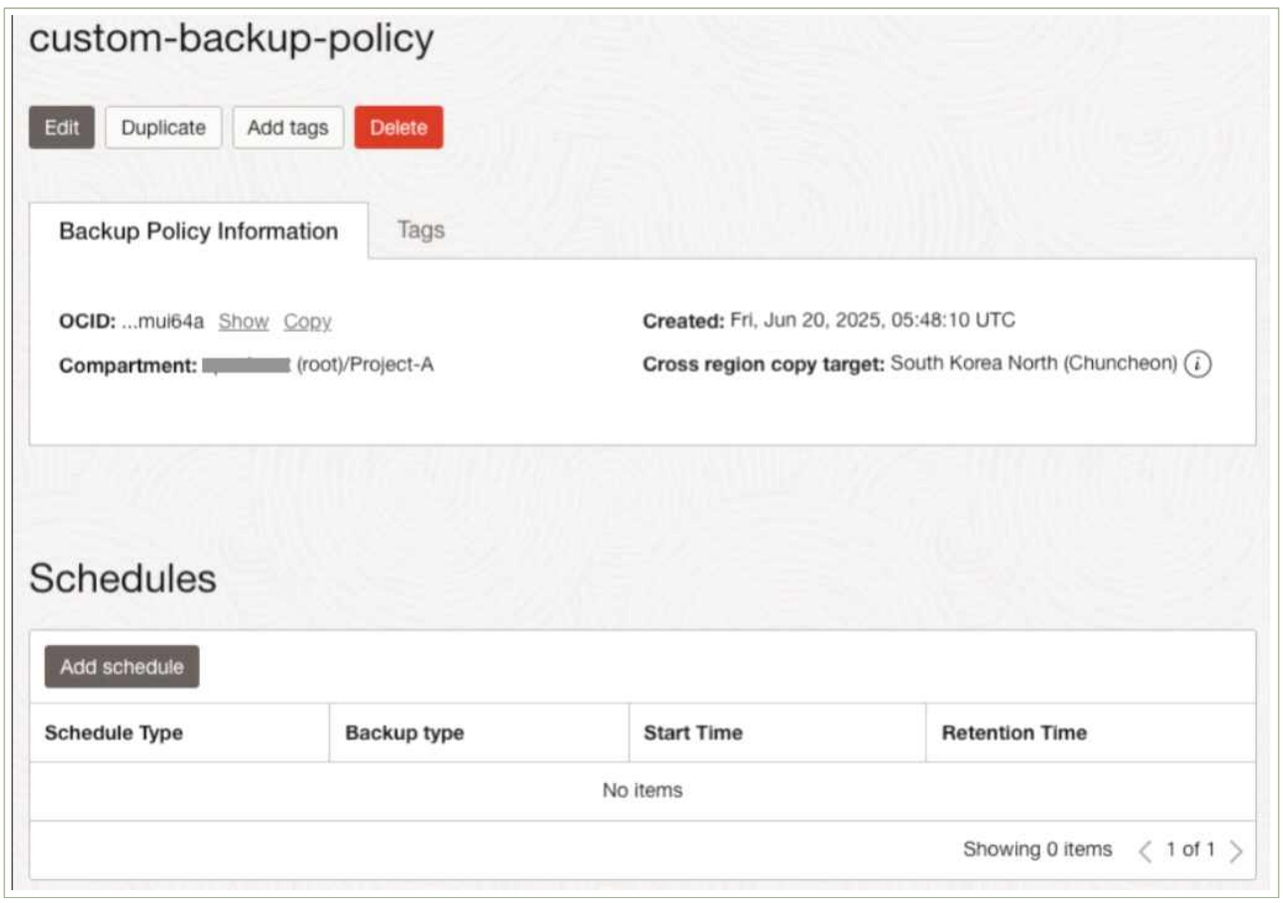
  (OCI 콘솔) '홈' → 'Storage' → 'Block Storage' → 'Backup Policies'

  OCI에서 기본으로 제공하는 백업 정책이 있으며, 필요하면 커스텀 정책을 추가할 수 있음

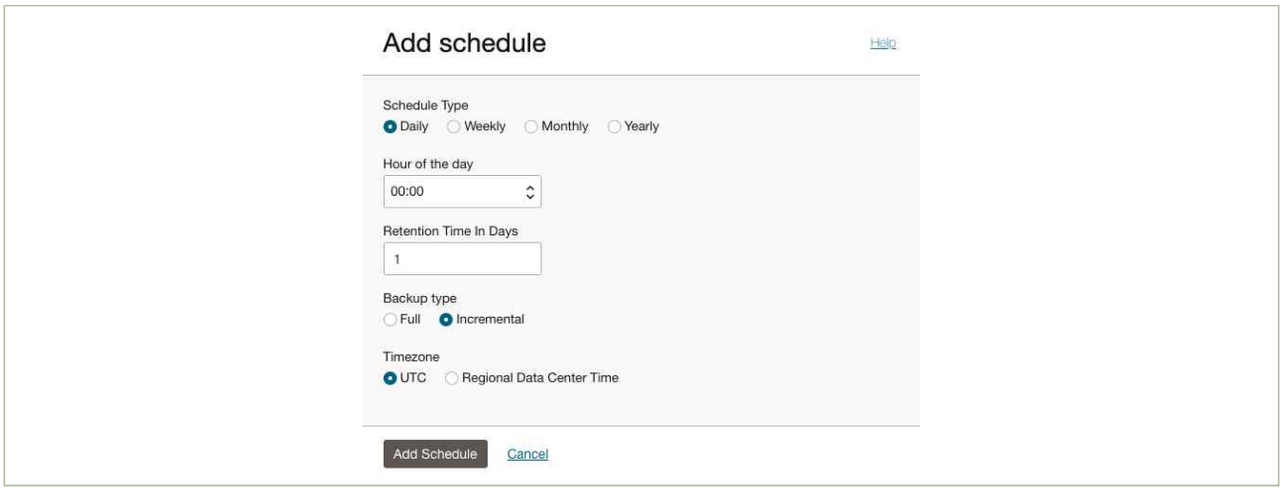


백업 정책	백업 주기	설명
Gold	일 단위	일일 증분 백업이 실행됩니다. 7일 동안 보존됩니다.
	주 단위	매주 일요일에 주 단위 증분 백업이 실행됩니다. 4주 동안 보존됩니다.
	월 단위	매월 첫날에 월간 증분 백업이 실행됩니다. 12개월 동안 유지됩니다.
	연 단위	매년 1월 1일에 전체 백업이 실행됩니다. 5년간 유지됩니다.
Silver	주 단위	매주 일요일에 주 단위 증분 백업이 실행됩니다. 4주 동안 보존됩니다.
	월 단위	매월 첫날에 월간 증분 백업이 실행됩니다. 12개월 동안 유지됩니다.
	연 단위	매년 1월 1일에 전체 백업이 실행됩니다. 5년간 유지됩니다.
Bronze	월 단위	매월 첫날에 월간 증분 백업이 실행됩니다. 12개월 동안 유지됩니다.
	연 단위	매년 1월 1일에 전체 백업이 실행됩니다. 5년간 유지됩니다.

- 커스텀 백업 주기 – 백업 정책에서 커스텀 정책을 추가하여, 원하는 백업 주기를 복수로 설정 가능함. 백업 시 Region 복제도 함께하도록 추가적으로 설정할 수 있음
  - (OCI 콘솔) '홈' → 'Storage' → 'Block Storage' → 'Backup Policies' 목록에서 새 Policy를 생성



- 원하는 스케줄을 추가로 생성



• 백업 담당자 지정

OCI IAM 정책으로 백업에 필요한 권한을 담당자에게 부여하고, Boot Volume을 포함한 Block Volume의 백업 및 Volume Group에 대한 권한을 부여

• 정책 샘플 예시

```
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
Allow group VolumeBackupAdmins to inspect volume-attachments in tenancy
Allow group VolumeBackupAdmins to inspect instances in tenancy
Allow group VolumeBackupAdmins to manage backup-policies in tenancy
Allow group VolumeBackupAdmins to manage backup-policy-assignments in tenancy
Allow group VolumeBackupAdmins to use volume-backups in tenancy where
request.permission='VOLUME_BACKUP_COPY'
```

(3) Database 백업

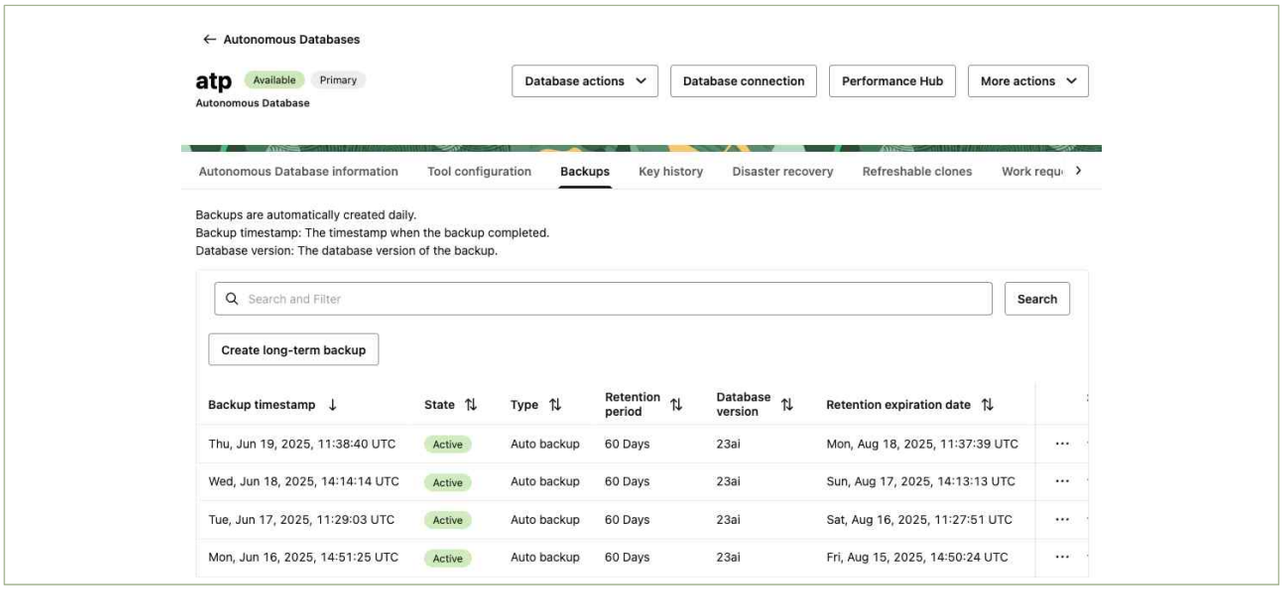
OCI에서 제공하는 각 Database 서비스에 따라 백업 관련 기능이 상이함

여기서는 대표적인 서비스인 OCI Autonomous Database를 기준으로 작성

• Autonomous Database

- 백업 주기

Autonomous Database는 자율 주행 데이터베이스로, 기본적으로 매일 자동 백업을 수행



- 백업 담당자 설정

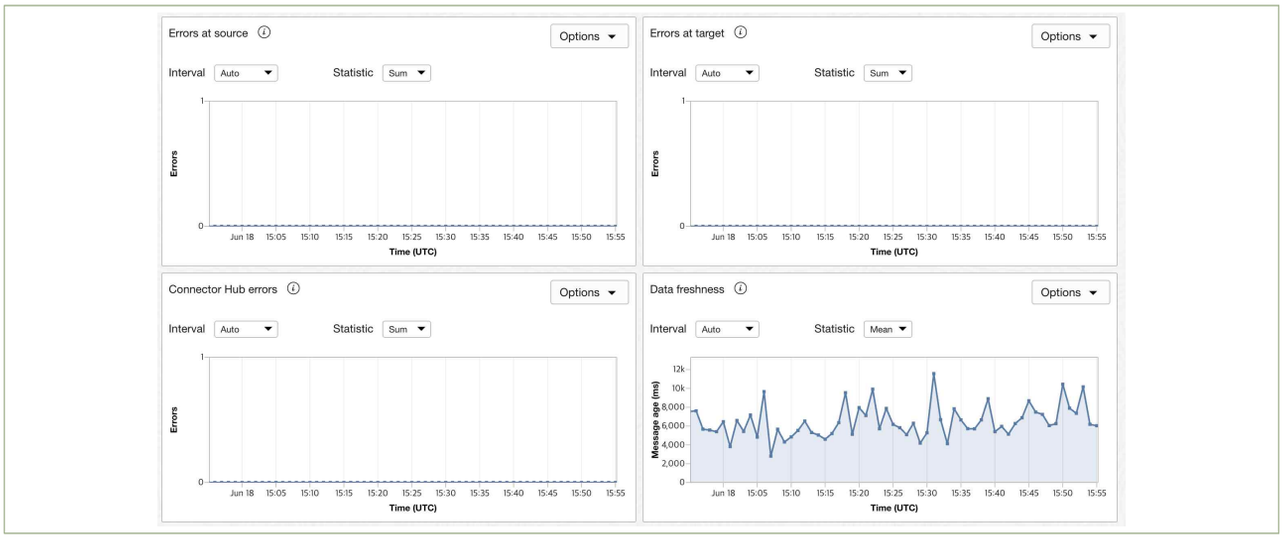
  OCI IAM 정책으로 백업에 필요한 권한을 담당자에게 부여

```
Allow group ADBBackupAdmins to manage autonomous-backups in tenancy
```

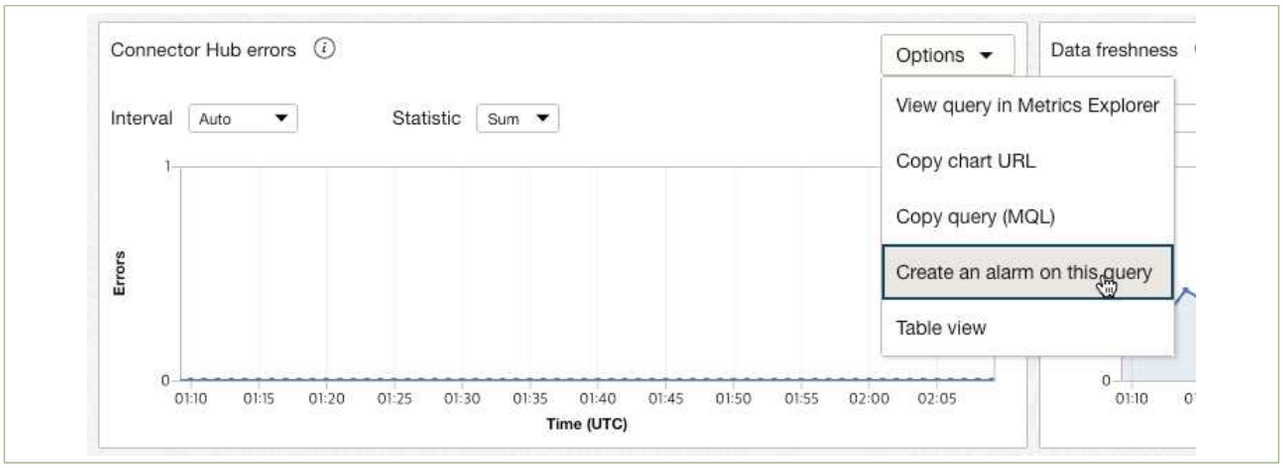
2) 주기적으로 백업 정상 여부에 대한 모니터링 및 검토

(1) Audit Log 백업

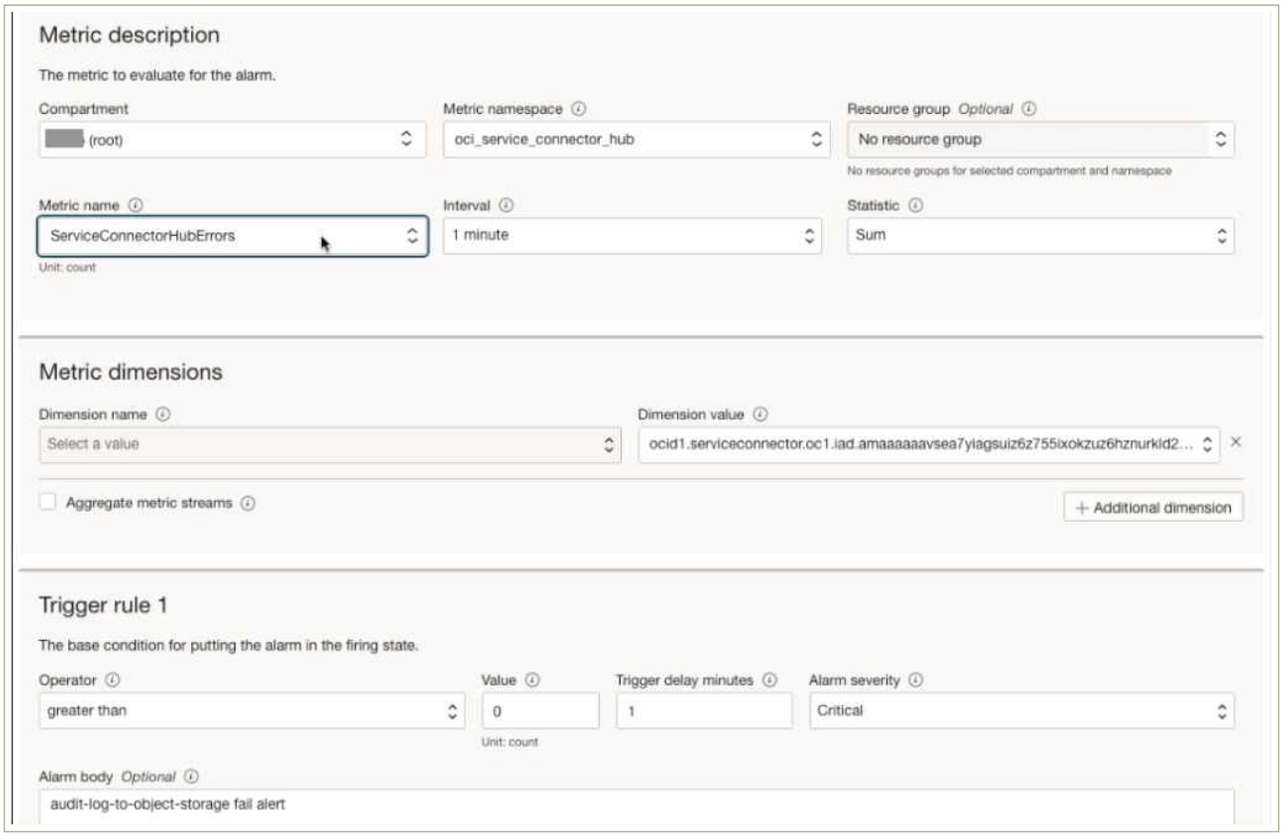
- Audit Log를 백업하는 Connector Hub의 메트릭에서 오류 발생 여부 확인 가능



• 모니터링을 위해 Connector Hub errors에 쿼리 알람 생성

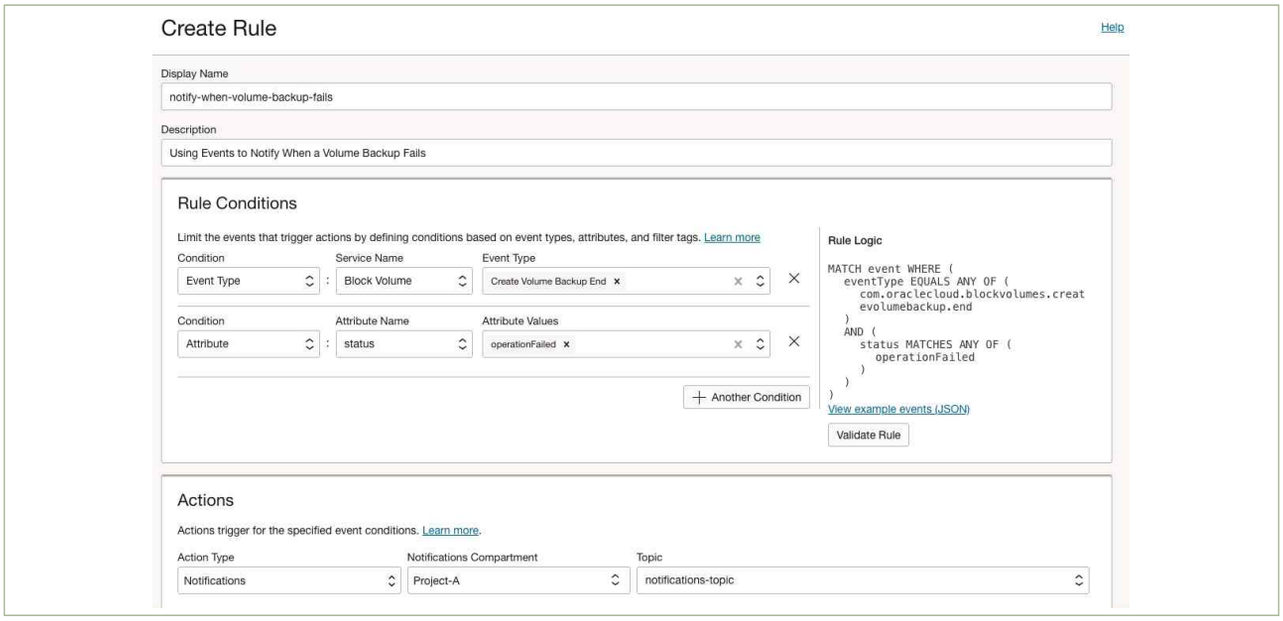


- 오류 발생 시 OCI Notification Topic으로 내역을 전송하며, 추가적으로 Notification Topic에 대한 구독 설정을 통해 이메일 등의 원하는 채널로 수신 가능



(2) Block Storage 백업

- Volume 백업 수행 시 관련 OCI Event가 발생
  - 백업이 성공하면, “Create Volume Backup End” 이벤트의 status 값이 operationSucceed이고, 실패하면 operationFailed이므로, operationFailed 발생 시 Notification Topic으로 관련 이벤트를 전송하도록 OCI Event Rule을 구성하여, 백업 오류시 담당자에게 통지되도록 설정



(3) Database 백업

- Autonomous Database
  - Autonomous Database는 자율 주행 데이터베이스이며, 관리형 서비스로 자동 백업 실패에 대해서 시스템에서 감지하여 처리

4 참고 사항

- Using Events to Notify When a Volume Backup Fails
  https://docs.oracle.com/en-us/iaas/Content/Block/Tasks/backupstatusevents.htm
- About Backup and Recovery on Autonomous Database
  https://docs.oracle.com/en-us/iaas/autonomous-database-serverless/doc/backup-intro.html

1 기준

식별번호	기준	내용
8.6	**백업 파일 원격 안전지역 보관**	금융회사는 전산 자료 등 중요도에 따라 중요도가 높은 파일에 대해선 원격 안전지역에 소산하여 보관하여야 한다.

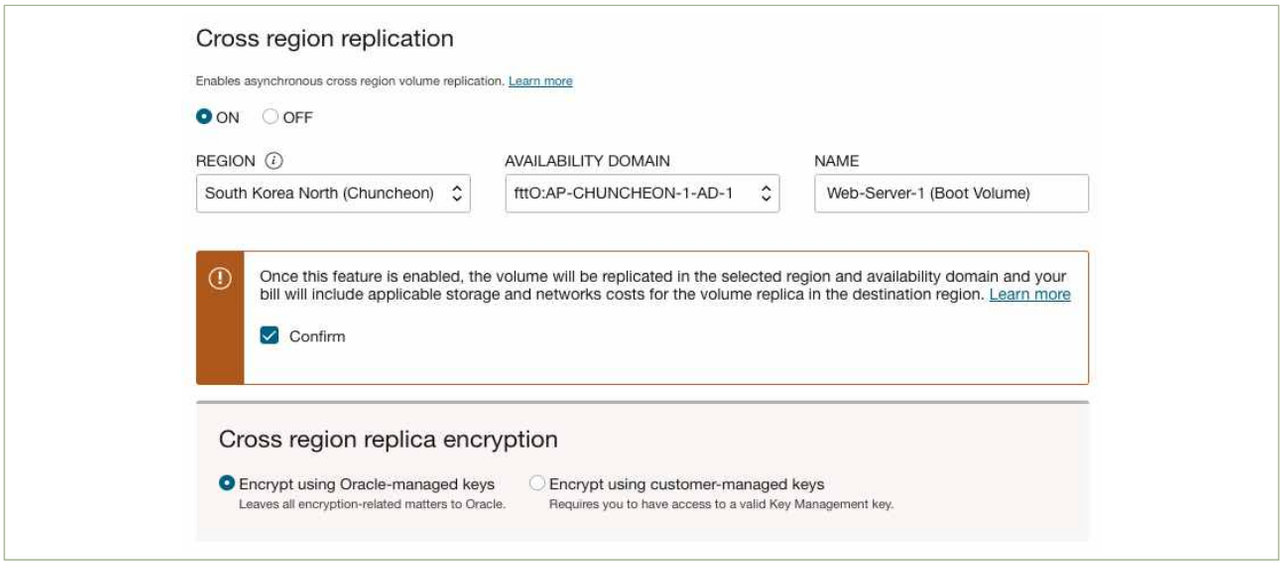
2 설명

- 금융회사는 중요도에 따라 전산 자료 등 중요가 높은 파일에 대해서는 원격 안전지역에 소산하여 보관하여야 한다.
  1) 클라우드 서비스 제공자의 DR 서비스 이용
  2) 금융회사 자체 데이터센터로 소산하여 보관 등

3 우수 사례

- “8.3 금융회사 전산 자료 백업”에서 명시된 “중요업무인 경우 클라우드 서비스와 관련한 중요 설정 파일 및 가상 시스템 이미지도 백업 대상”을 근거로 여기서 소산되는 대상은 Block Volume, Object Storage에 있는 자료라고 가정
  1) 클라우드 서비스 제공자의 DR 서비스 이용
    (1) 소산 대상에 각 OCI 서비스에서 제공하는 기능을 통해 원격 안전지역으로 복제
      • Block Storage
        서버의 Boot Volume 및 Block Volume에 대한 원격 복제 기능을 사용하여 원격지로 소산
        - (OCI 콘솔) ‘홈’ → ‘Storage’ → ‘Block Storage’ → ‘Boot Volumes’ 또는 ‘Block Volumes’ 에서 백업 대상 Volume으로 이동 Block Storage → Boot Volumes / Block Volumes 에서 백업 대상 Volume으로 이동
        - Cross region replication을 설정 (국내 리전 기준으로 복제 목적지로 사용할 수 있는 원격 안전지역 리전을 참고하여 설정)

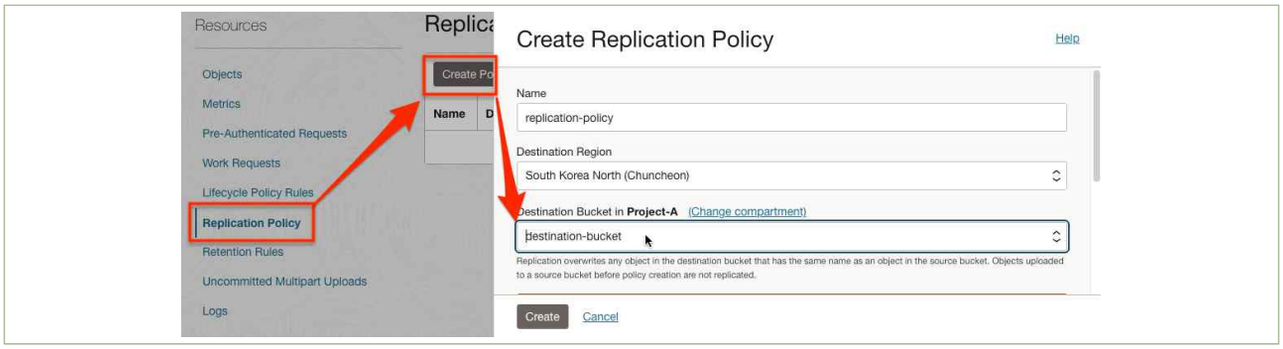
Source Region	Destination Region
South Korea Central (Seoul)	Japan Central (Osaka) Japan East (Tokyo) South Korea North (Chuncheon)
South Korea North (Chuncheon)	Japan Central (Osaka) Japan East (Tokyo) South Korea Central (Seoul)



- Object Storage(데이터베이스 백업 포함)

  데이터베이스 백업 또는 사용자가 중요 설정 파일은 Object Storage로 백업을 한 경우, 또는 3rd Party 백업 툴을 사용해 Object Storage에 백업한 경우 등을 포함하여 Object Storage에 있는 자원에 대한 원격지 보관이 필요한 경우, Object Storage 서비스의 리전 간 복제 기능을 사용하여 원격지로 소산 가능

  - (OCI 콘솔) '홈' → 'Storage' → 'Object Storage & Archive Storage' → 'Bucket'에서 대상 Bucket으로 이동 Storage → Object Storage & Archive Storage → Bucket에서 대상 Bucket으로 이동
  - Replication Policy에서 새 복제 정책을 생성하여 타 리전으로 복제



2) 금융회사 자체 데이터센터로 소산하여 보관

(1) Block Storage

OCI에서 제공하는 Block Storage 서비스의 백업 기능으로 생성된 백업한 파일은 사용자가 직접 다운로드 불가하며, 대안으로 먼저 OCI Object Storage에 백업하고, 다시 자체 데이터센터로 이전하는 방안을 사용

• 1안) OCI CLI Object Storage sync 방식

Block Storage 파일시스템 내 파일을 OCI CLI의 Object Storage sync 기능으로 지정한 Object Storage에 복사하고, Object Storage에서 자체 데이터센터로 다운로드하는 방법

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Domains' → 'Default Domain'을 클릭 → Dynamic Group 생성 (Object Storage 접근 목적) Identity & Security → Domains → Default Domain을 클릭합니다. Dynamic Group 탭으로 이동하여, Object Storage 접근을 위해 Dynamic Group을 생성합니다.

```
Name: instance-dg
All {instance.compartment.id = {YOUR_COMPARTMENT_OCID_OF_OBJECT_STORAGE}'}
```

- (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' → 'IAM Policy' 생성

```
Allow dynamic-group Default/instance-dg to manage objects in compartment
{YOUR_COMPARTMENT_NAME}
```

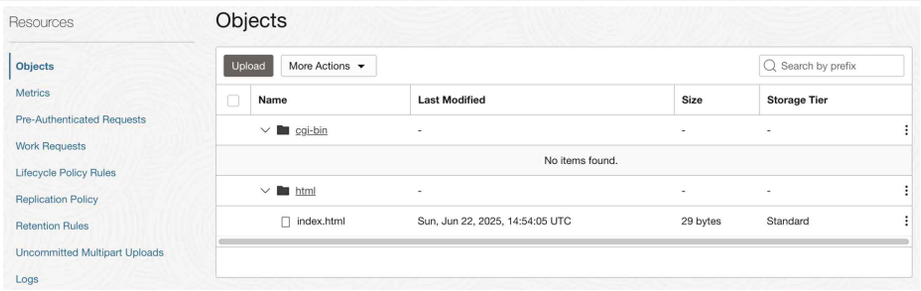
- (OCI 콘솔) '홈' → 'Storage' → 'Object Storage & Archive Storage' → 'Bucket' → Bucket 생성 (예, backup-bucket)
- 백업 대상의 Boot/Block Volume이 연결된 Compute 인스턴스에 SSH로 접속
- oci cli를 설치 (참조 - https://github.com/oracle/oci-cli)
- 환경 변수 설정

```
OCI_CLI_AUTH=instance_principal
```

- OCI CLI 명령어(oci os object sync)로 파일시스템 지정한 경로(--src-dir) 하위에 저장된 파일을 지정한 Bucket으로 동기화

```
oci os object sync -bn backup-bucket --src-dir /var/www
```

Object Storage Bucket에서 동기화 결과 확인



- 필요 시, crontab에 등록하여 주기적으로 실행되도록 구성

- 2안) rclone 방식

  rclone을 사용하여, Object Storage로 복사하고, Object Storage에서 다시 자체 데이터센터로 다운로드하는 방법

  - (OCI 콘솔) '홈' → 'Identity & Security' → 'Domains' → 'Default Domain'을 클릭 → Dynamic Group 생성 (Object Storage 접근 목적)

```
Name: instance-dg
All {instance.compartment.id = {YOUR_COMPARTMENT_OCID_OF_OBJECT_STORAGE}'}
```

  - (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' → 'IAM Policy' 생성

```
Allow dynamic-group Default/instance-dg to manage objects in compartment
{YOUR_COMPARTMENT_NAME}
```

  - (OCI 콘솔) '홈' → 'Storage' → 'Object Storage & Archive Storage' → 'Bucket' → Bucket 생성 (예, backup-bucket)- (OCI 콘솔) '홈' → Storage → Object Storage & Archive Storage → Bucket으로 이동하여, 사용할 Bucket을 만듭니다. 예, backup-bucket
  - 백업 대상의 Boot/Block Volume이 연결된 Compute 인스턴스에 SSH로 접속
  - rclone 설치 (참고 - https://rclone.org/install/)

```
sudo -v ; curl https://rclone.org/install.sh | sudo bash
```

  - rclone config로 OCI Object Storage 연결 성구

```
rclone config

No remotes found, make a new one?
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n

Enter name for new remote.
name> oci-os

Option Storage.
Type of storage to configure.

41 / Oracle Cloud Infrastructure Object Storage
```

```
    \ (oracleobjectstorage)

Storage> 41

Option provider.
Choose your Auth Provider
...
 3 | each instance has its own identity, and authenticates using the certificates that are
read from instance metadata.
...
provider> 3

Option namespace.
Object storage namespace
Enter a value.
namespace> {YOUR_OBJECT_STORAGE_NAMESPACE}

Option compartment.
Specify compartment OCID, if you need to list buckets.
List objects works without compartment OCID.
Enter a value. Press Enter to leave empty.
compartment> {YOUR_COMPARTMENT_OCID_OF_OBJECT_STORAGE}

Option region.
Object storage Region
Enter a value.
region> ap-seoul-1

Option endpoint.
Endpoint for Object storage API.
Leave blank to use the default endpoint for the region.
Enter a value. Press Enter to leave empty.
endpoint>

Edit advanced config?
y) Yes
n) No (default)
y/n> n

Configuration complete.
...
```

```
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d> y

...
q) Quit config
e/n/d/r/c/s/q> q
```

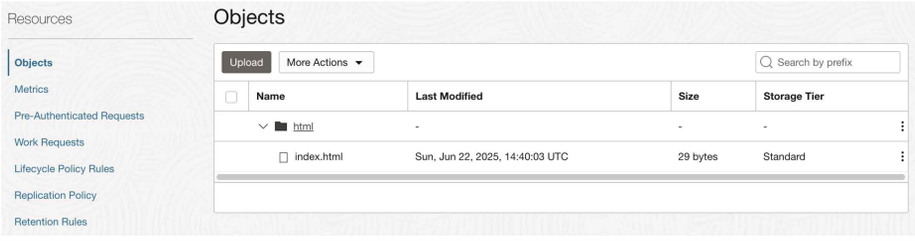
- Bucket 내 오브젝트를 조회하여, Object storage와 연결 확인

```
rclone ls oci-os:backup-bucket
```

- rclone sync 명령어로 대상 폴더를 Object Storage로 동기화

```
rclone sync /var/www oci-os:backup-bucket
```

- 동기화가 완료 후, Object Storage에서 결과 확인



- 필요 시, crontab에 등록하여 주기적으로 실행되도록 구성

• 3안) Commvault 등 외부 백업 솔루션을 사용하여 백업

(2) Object Storage

자체 데이터센터에서 OCI 환경으로 접근이 가능한 경우, Object Storage에 있는 백업을 다운로드하는 방법

• 예시, 자체 데이터센터 내 리눅스 환경

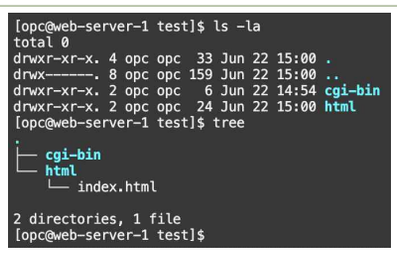
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Domains' → 'Default Domain' → IAM User 생성
- API 호출을 위한 API Key 등록
- (OCI 콘솔) '홈' → 'Identity & Security' → 'Policies' → 'IAM Policy 생성' (해당 User의 Object Storage에 대한 권한 부여)

```
Allow group Default/test-user-group to manage objects in compartment
{YOUR_COMPARTMENT_NAME}
```

- 자체 데이터센터 내 리눅스 서버에 SSH로 접속
- oci cli 설치 (참조 - https://github.com/oracle/oci-cli)
- API 호출을 위한 API Key 등록
- OCI CLI 명령어(oci os object sync)로 Bucket을 현재 경로로 동기화

```
oci os object sync -bn backup-bucket --dest-dir .
```

- 동기화 완료 후, 현재 폴더 확인



- 필요 시, crontab에 등록하여 주기적으로 실행되도록 구성

(3) Database 백업

• Autonomous Database

- Autonomous Database에서 관리형 서비스 제공하는 자동 백업은 사용자가 직접 다운로드 불가능. 자체 데이터센터로 백업을 원하는 경우, Data Pump 사용
- sqlplus 및 data pump 설치 필요 (예: OCI CloudShell 사용)
- (OCI 콘솔) '홈' → 'Oracle Database' → 'Autonomous' → 백업 대상 데이터베이스로 이동 → Database connection 메뉴에서 Wallet 파일 다운로드
- 다운로드한 Wallet 파일을 압축 해제

```
mkdir -p ~/wallet_atp
unzip Wallet_atp.zip -d ~/wallet_atp
```

- sqlnet.ora 파일의 DIRECTORY를 sqlnet.ora이 속한 폴더로 수정

```
WALLET_LOCATION = (SOURCE = (METHOD = file) (METHOD_DATA =
(DIRECTORY="/home/kildong/wallet_atp")))
SSL_SERVER_DN_MATCH=yes
```

- sqlplus 접속 테스트

```
sqlplus admin@atp_low
```

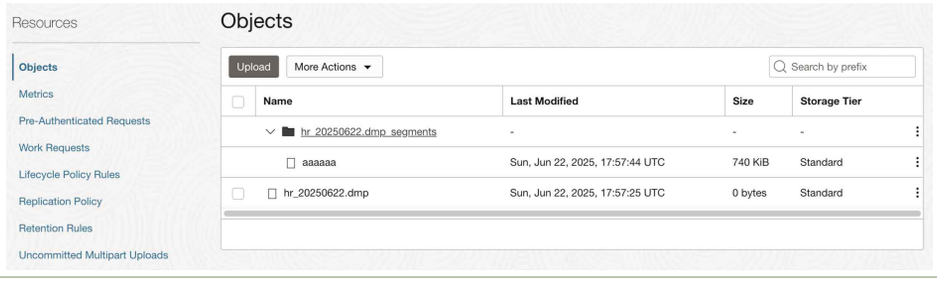
- 데이터베이스 유저가 Object Storage에 연결 시 사용할 Credential을 생성
- OCI IAM User와 해당 유저의 Auth Token으로 Credential을 생성

```
BEGIN
  DBMS_CLOUD.CREATE_CREDENTIAL(
    credential_name => 'DEMO_CRED',
    username => 'default/kildong.hong@example.com',
    password => '{AUTH_TOKEN}' );
END;
/
```

- Data Pump로 Export 실행 (예: hr 스키마를 백업, dumpfile에 경로에 Object Storage Bucket 지정)

```
expdp admin/<DB_PASSWORD> @atp_low credential=DEMO_CRED schemas=hr
dumpfile=https://objectstorage.ap-seoul-1.oraclecloud.com/n/{OBJECT_STORAGE_NA
MESPACE}/b/backup-bucket/o/hr_20250623.dmp logfile=hr_20250623.log
directory=data_pump_dir parallel=4
```

- (OCI 콘솔) '홈' → 'Storage' → 'Object Storage & Archive Storage' → 'Bucket' 해당 Bucket으로 이동하여 Export 결과를 확인



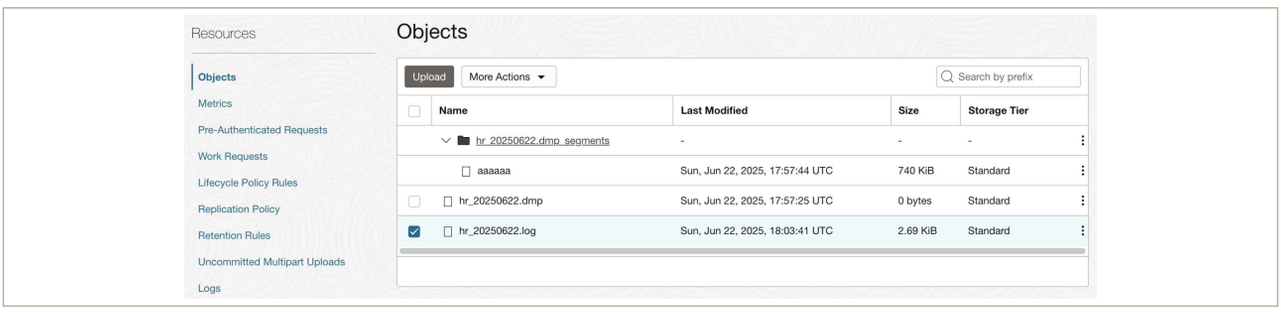
- Export 로그 확인

```
SELECT object_name, created FROM DBMS_CLOUD.LIST_FILES('DATA_PUMP_DIR');
```

- Export 로그 확인 후, 필요 시 추가로 Object Storage에 업로드

```
BEGIN
DBMS_CLOUD.PUT_OBJECT(credential_name => 'DEMO_CRED',
      object_uri =>
https://objectstorage.ap-seoul-1.oraclecloud.com/n/{OBJECT_STORAGE_NAMESPACE}/
b/backup-bucket/o/hr_20250622.log',
      directory_name => 'DATA_PUMP_DIR',
      file_name => 'hr_20250622.log');
END;
/
```

- (OCI 콘솔) '홈' → 'Storage' → 'Object Storage & Archive Storage' → 'Bucket' 으로 이동하여 결과 확인



- Object Storage 내 백업 파일은 Object Storage 다운로드 절차를 거쳐 자체 데이터센터로 이전

4 참고 사항

- Replicating a Volume

  https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/volumereplication.htm

1 기준

식별번호	기준	내용
8.7	**주요 전산장비 이중화**	금융회사는 클라우드 환경을 통한 인프라 구성 시 주요 전산장비를 이중화 하여야 한다.

2 설명

- 금융회사는 클라우드 환경을 통한 인프라 구성 시 가상화 기능을 이용하여 주요 전산장비를 이중화하여야 한다.
  1) 클라우드 가상화 기능을 이용하여 주요 전산장비(서버, 데이터베이스 등) 이중화 구성
  2) 이중화 구성 시 원격 안전지역 등을 고려

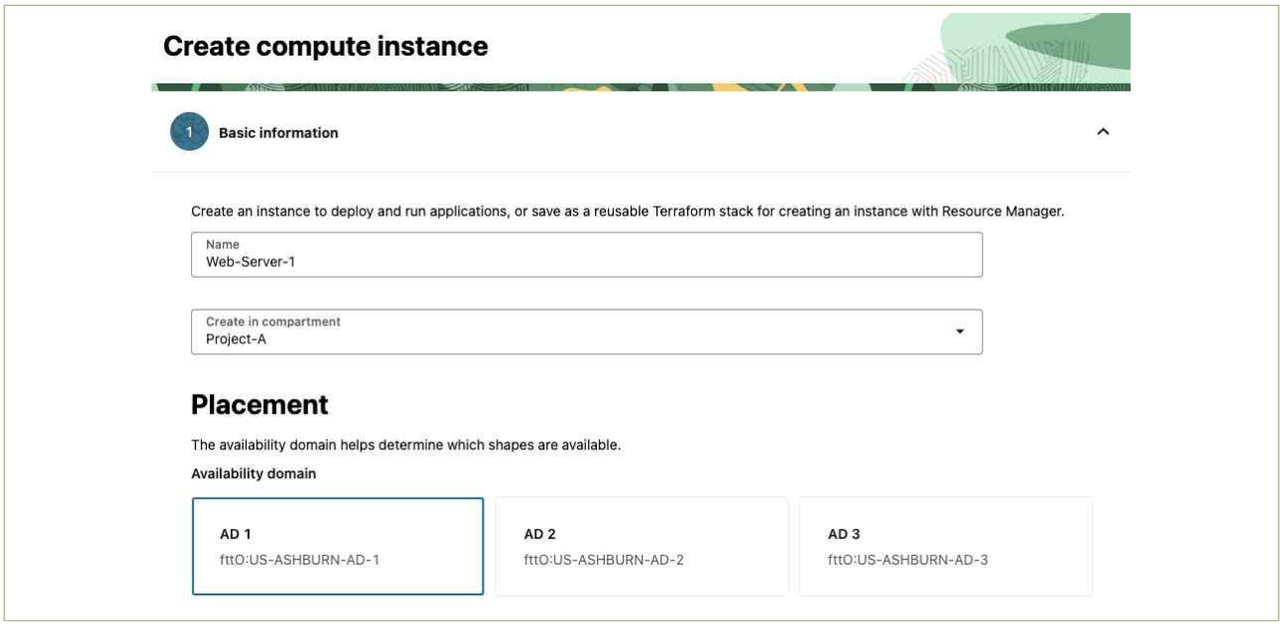
3 우수 사례

1) 클라우드 가상화 기능을 이용하여 주요 전산장비(서버, 데이터베이스 등) 이중화 구성

OCI에서는 서버, 데이터베이스, 네트워크, 스토리지 등의 레벨에서 고가용성을 보장하기 위한 다양한 기능을 제공

(1) 서버 이중화

- 멀티 Availability Domain(AD) 기반 이중화
  - Availability Domain(AD)는 OCI 리전 내에서 서로 독립된 데이터센터
  - 멀티 AD를 지원하는 리전에서는 서버를 서로 다른 AD에 배치하여 이중화 구성



- 멀티 Fault Domain 기반 이중화
  - 단일 AD 내에는 3개의 FD가 존재하며, 이는 하드웨어 장애나 유지 보수로 인한 영향을 최소화하기 위한 구조
  - 단일 AD를 보유한 리전에서는 서버를 서로 다른 FD에 배치하여 이중화 구성
  - 별도 지정하지 않으면 서버는 배포 시 AD 내 3개 FD에 균등하게 분산 구성

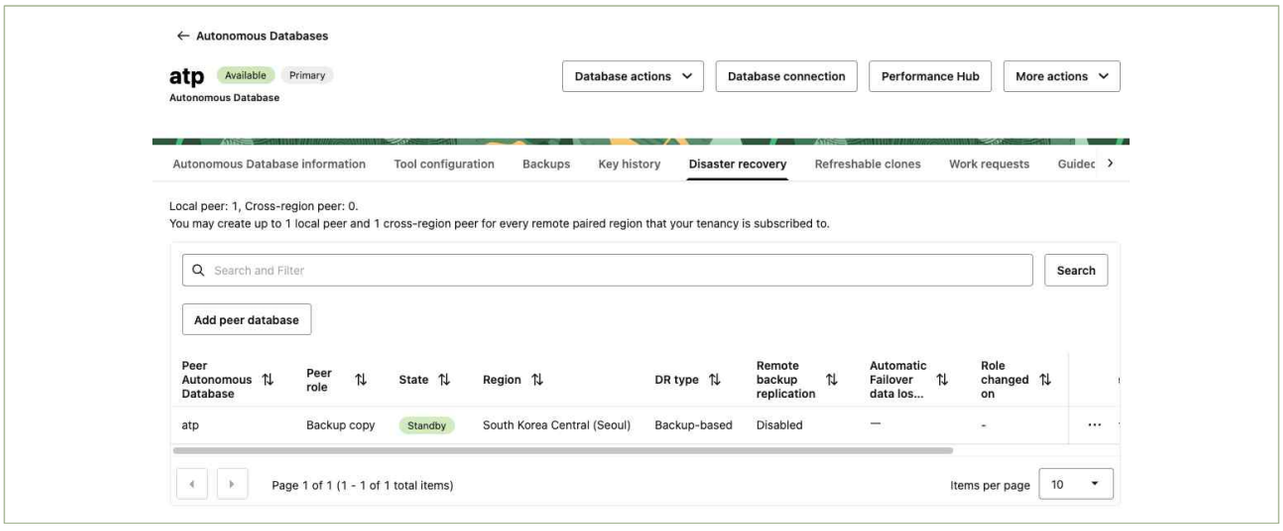
- Load Balancer 이중화
  - OCI Load Balancer를 통해 이중화된 서버로 트래픽 분배
  - OCI Load Balancer를 통해 이중화된 서버로 트래픽을 분배합니다.
  - OCI Load Balancer는 기본적으로 멀티 AD 또는 단일 AD 환경에서 멀티 FD 기반 내부 이중화 제공별도의 추가 작업 불필요

(2) 데이터베이스 이중화

OCI에서 제공하는 각 Database 서비스에 따라 백업 관련 기능은 상이하며, 여기서는 대표적인 서비스인 OCI Autonomous Database를 기준으로 작성

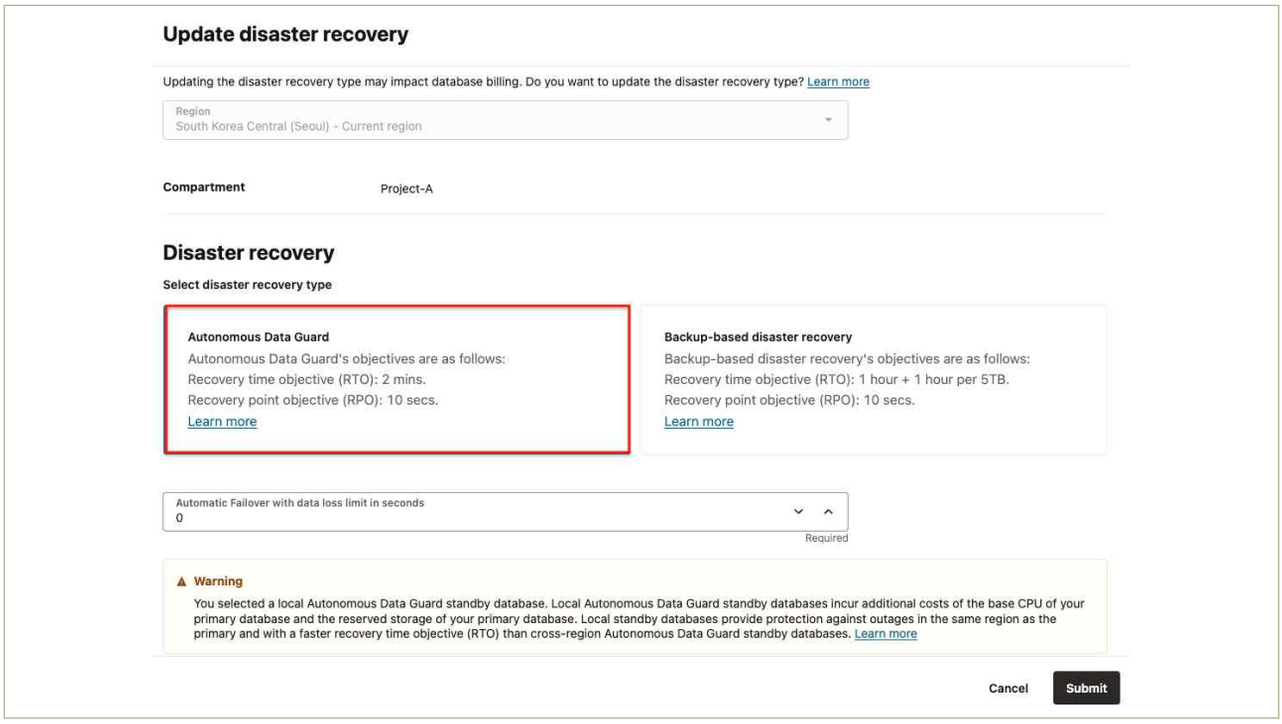
• Oracle Autonomous Database

- 기본 HA 제공, 생성 시 Local Peer 기반 DR 구성



• Oracle Data Guard

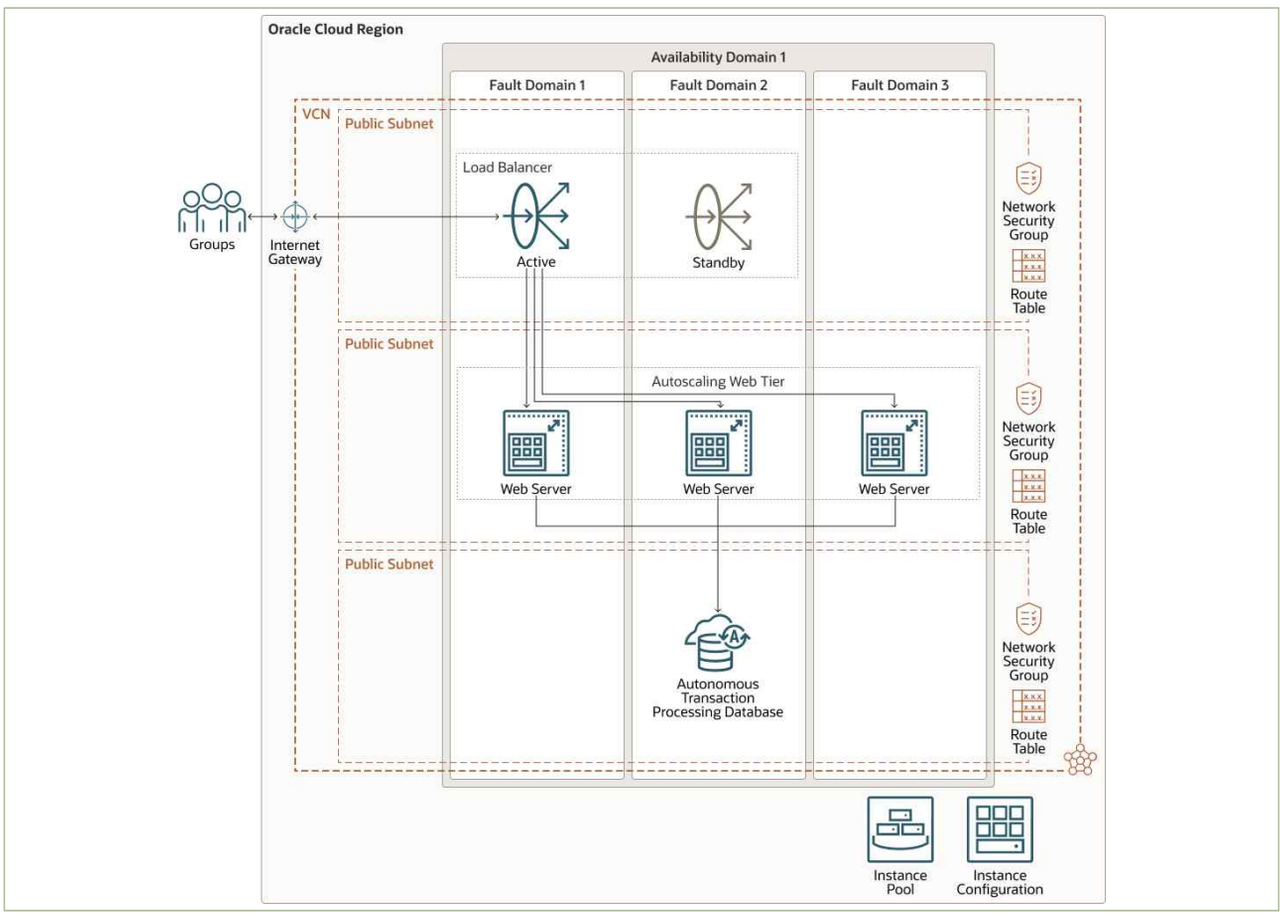
- DataGuard를 활성화하면, Primary–Standby 간 실시간 복제를 통해 자동 장애 전환(Failover) 제공
- 단일 리전 내 생성한 Autonomous Database에 대해 백업 기반의 기본 Disaster Recovery 방식을 Data Guard 형식으로 변경하는 경우, RTO·RPO 단축 가능하나 추가 비용 발생



- Oracle RAC (Real Application Clusters)
  - 멀티 데이터베이스 노드에 대한 Active-Active HA 제공
  - Autonomous Database는 고가용성과 무중단 운영을 위해 내부적으로 Oracle RAC 사용
  - OCI Base Database Service에서는 Enterprise Edition Extreme Performance edition에서 2 노드 RAC를 지원하나, 관리형 서비스로 사용자가 RAC 노드나 설정에 직접 접근 불가
  - Base Database Service에서는 사용자가 RAC 노드나 설정에 접근 가능

(3) 이중화 구성 예시

요구사항에 따라 이중화 구성은 다양하게 적용할 수 있으며, 웹 서버나 Autonomous Database와 Load Balancer를 사용하는 간단한 구성인 경우, OCI에서 제공하는 이중화 기능을 통해 아래 그림과 같이 이중화 가능



2) 이중화 구성 시 원격 안전지역 등을 고려

(1) 원격 안전 지역

- 주센터와 재해복구 센터 사이에 대한 명시적 기준은 없으나, 한국정보통신기술협회의 정보시스템 재해복구 지침에서는 재해복구 센터의 위치 선정 시의 고려 사항 항목 중, 동일 재해 영향권 위험성 항목에서 "주 센터와 재해복구 센터는 동일한 지리적 위험을 갖는 지역(예, 지진대, 홍수권역 등)에 위치하지 않아야 한다. 이는 대개의 경우 15~80km 정도의 거리이면 달성할 수 있나 지역적 특성에 따라 달라질 수 있다"라고 명시

• OCI는 Dual Region(Two Region) 전략을 통해 단일 국가 또는 지역 내에 2개의 리전을 구축하고 있으며, 해당 전략에 따라 OCI는 한국에 서울, 춘천 2개의 리전을 보유

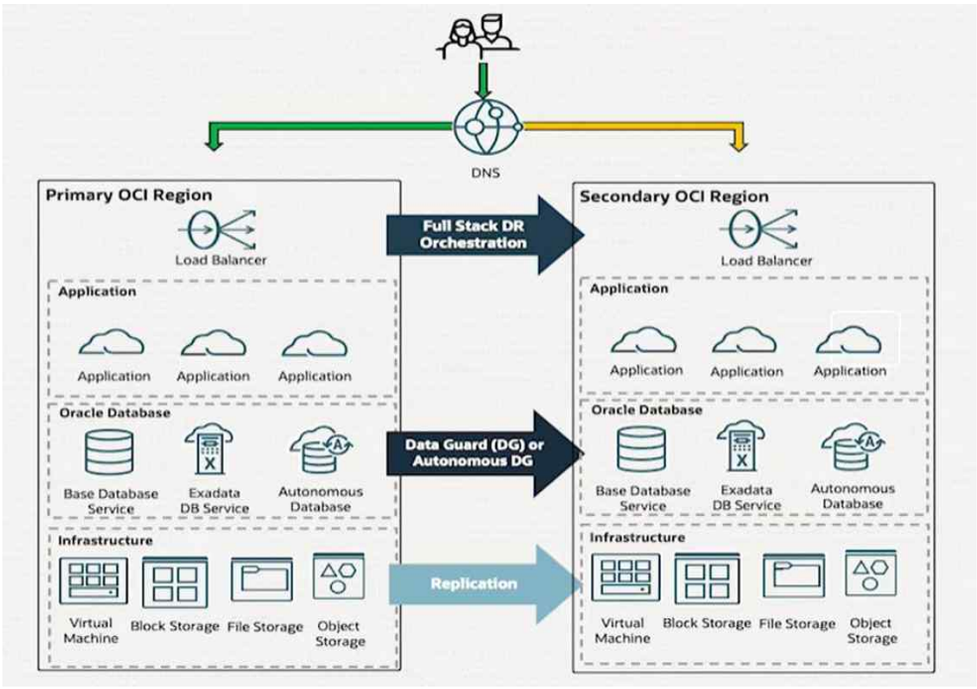
(2) 리전간 이중화 구성

• OCI 서비스 별 제공하는 DR 서비스

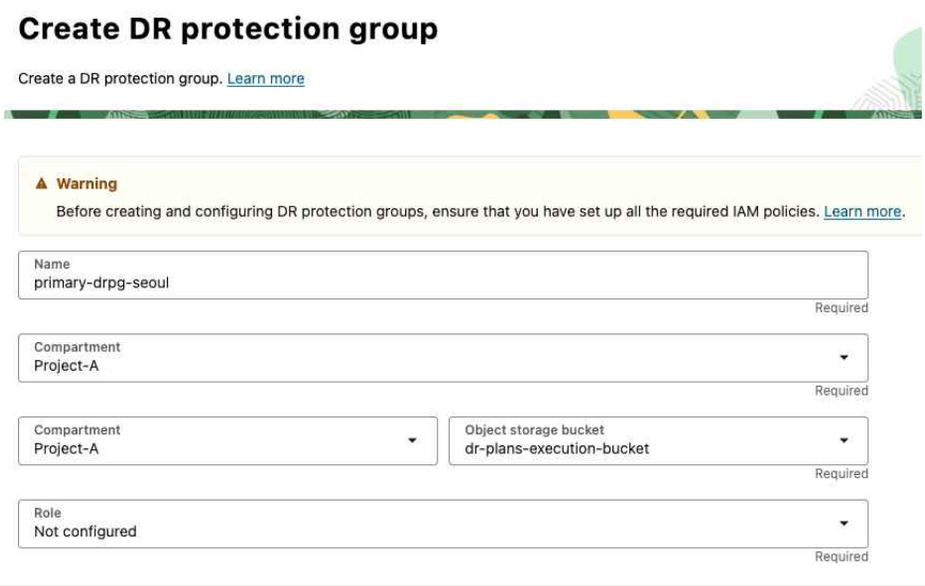
OCI 서비스	주요 기능
Object Storage 리전간 복제	리전간에 Object Storage를 복제함
Block Volume 복제	Primary, DR 리전간 Block Volume을 복제함
Oracle Data Guard	DR 리전에 StandBy 데이터베이스를 생성
Oracle Golden Gate	리전간 데이터베이스를 실시간 복제
Traffic Management (DNS Steering)	장애시 DR 사이트로 트래픽 자동 전환
FastConnect & VPN	On-Premise와 OCI간 연결 이중화
DB Autonomous Recovery Service	데이터 손실 없는 백업

• Full Stack DR 서비스

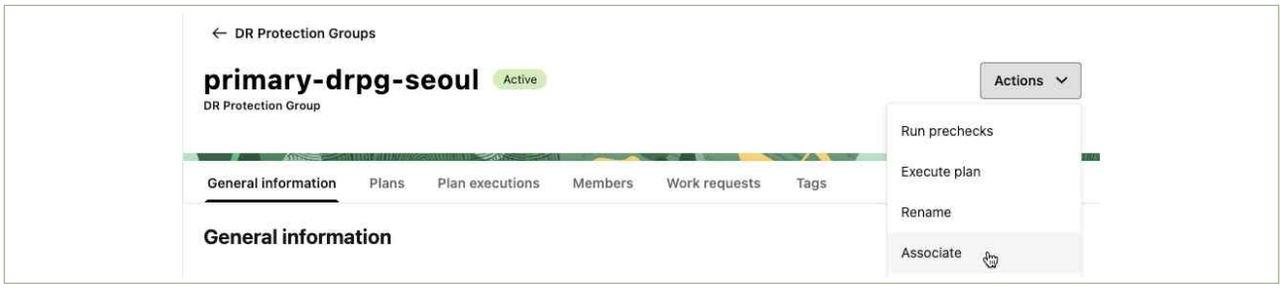
Full Stack DR은 완전 관리형 서비스로 OCI 리전 간에 서버, 데이터베이스, Load Balancer 등 여러 계층에서 DR을 구성이 가능



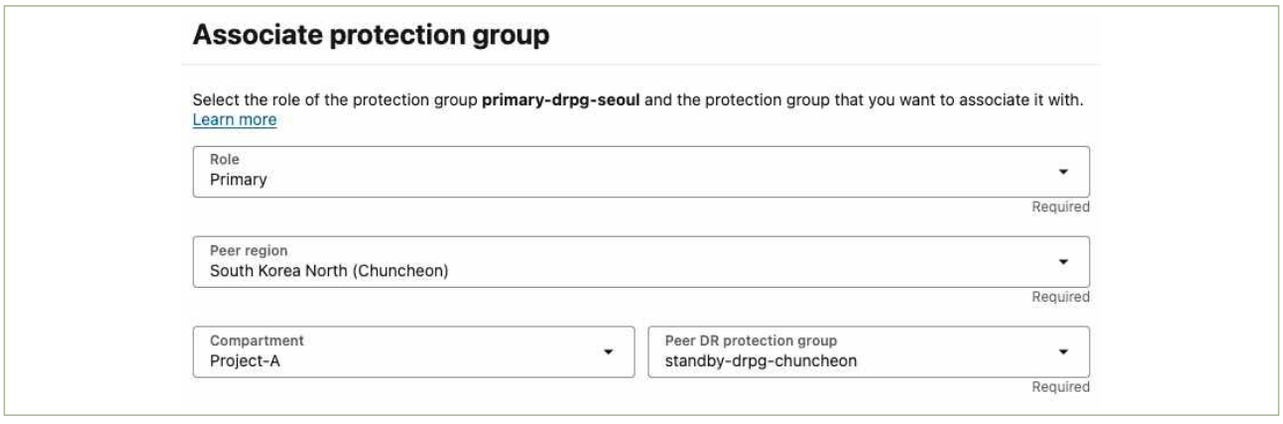
- (OCI 콘솔) '홈' → 'Migration and Disaster Recovery' → 'Disaster Recovery' → 'DR Protection Groups' → DR protection group 생성



- Standby 리전에서도 같은 방법으로 DR protection group 생성
- Primary 리전의 DR protection group에서 오른쪽 위 Actions 메뉴의 Associate를 선택

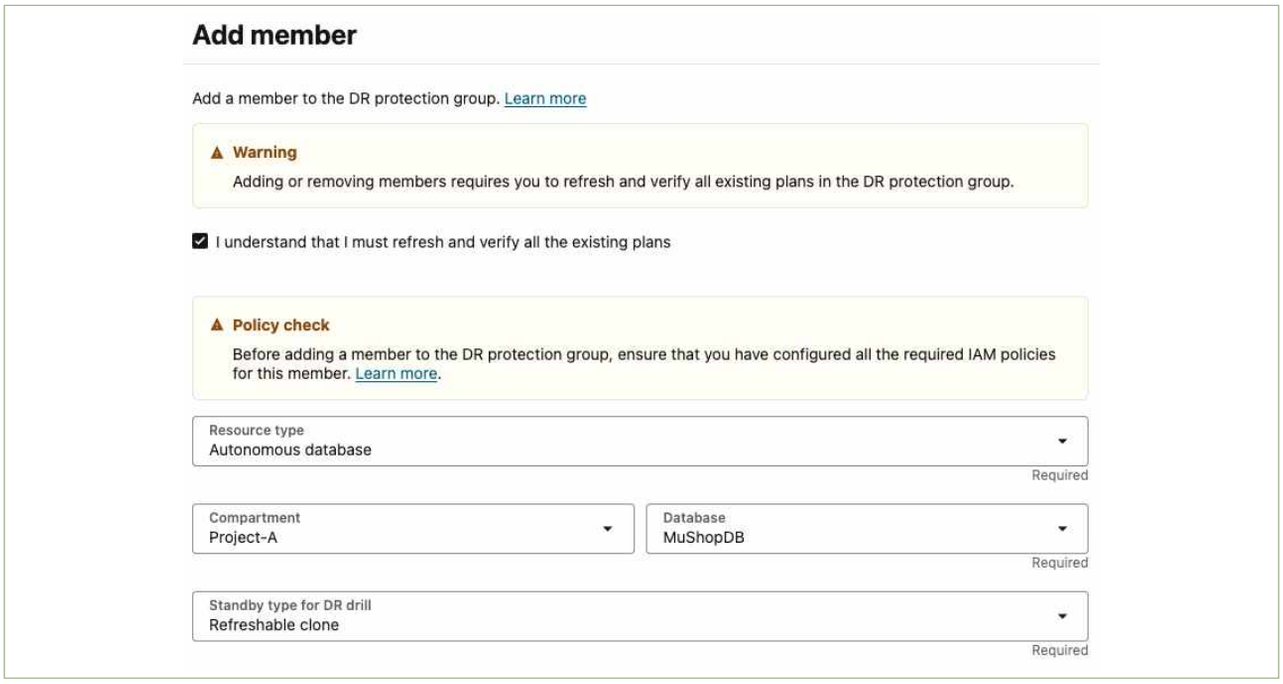


- 선택한 그룹의 Role을 Primary로 지정
- Peer region으로 Standby 리전을 선택하고, 매핑되는 DR protection group을 지정

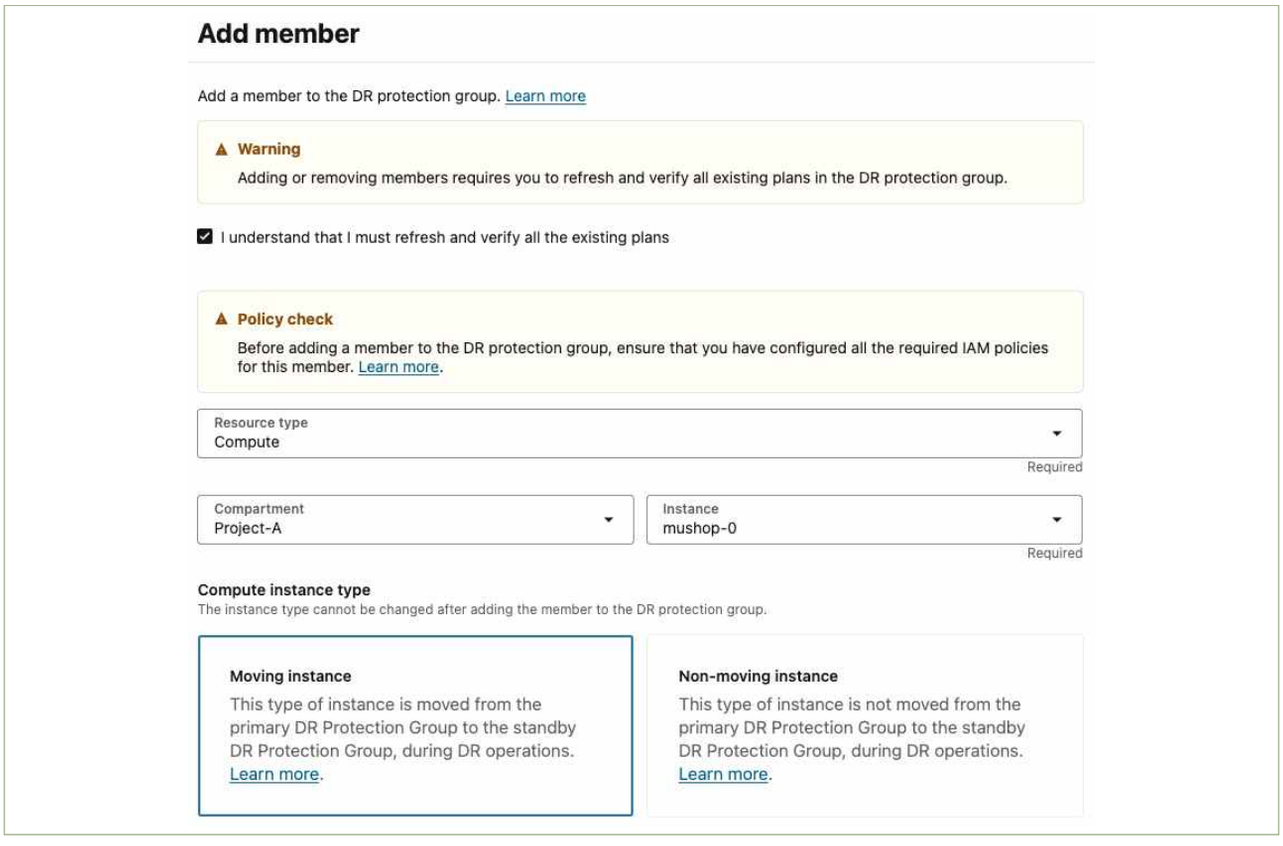


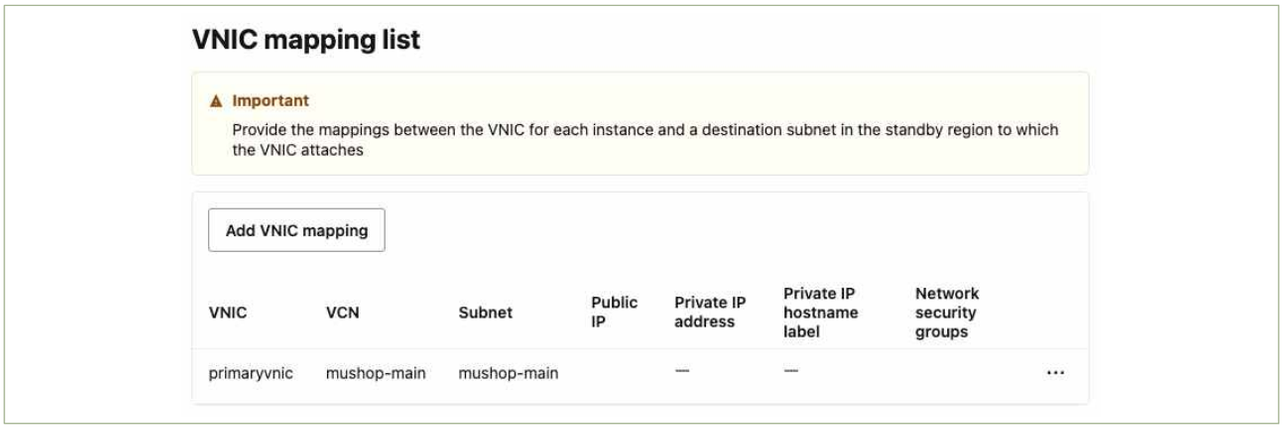
- 업데이트가 완료 후, Standby 리전에 있는 DR protection group이 업데이트 되었는지 점검

- Primary 리전으로 돌아가서, DR protection group에서 Members 탭을 클릭하여 멤버 추가 → Autonomous Database 추가

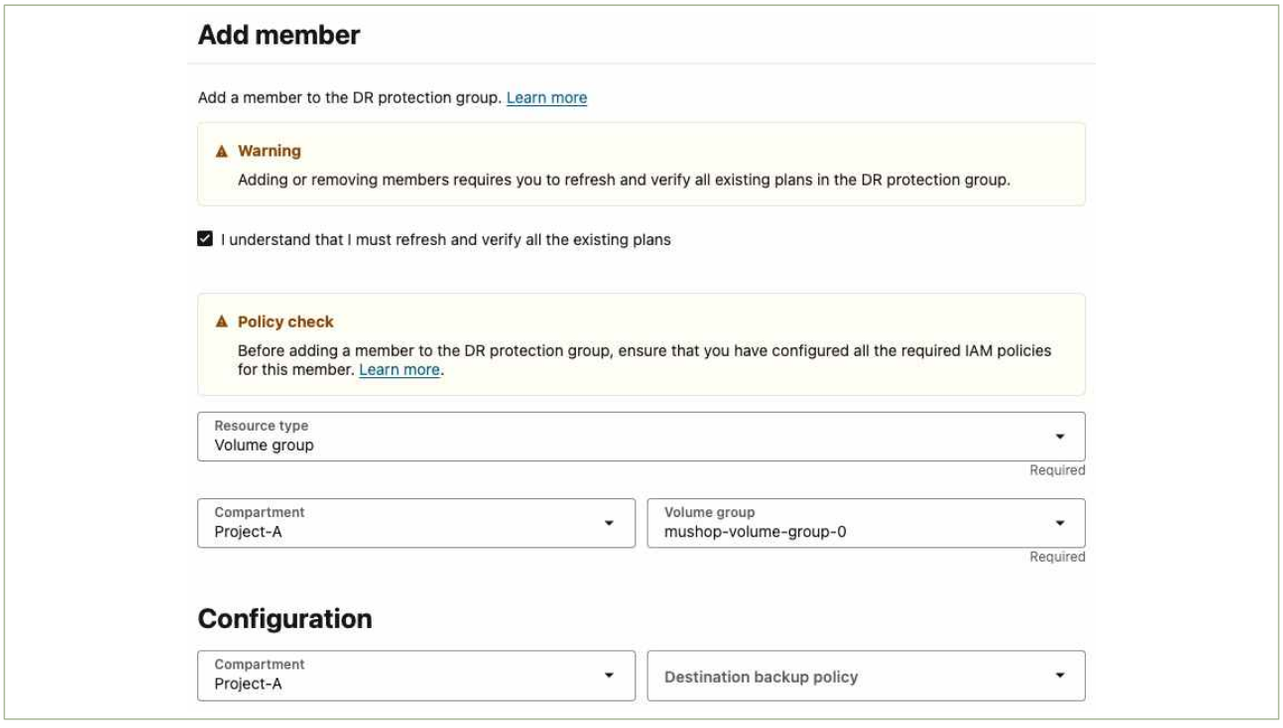


- 서버 추가: Compute 인스턴스를 추가하고, 인스턴스의 VNIC이 Standby 리전 에서 사용할 VCN, 서브넷을 지정 (다수의 서버에 대해 동일한 방식으로 적용 가능)

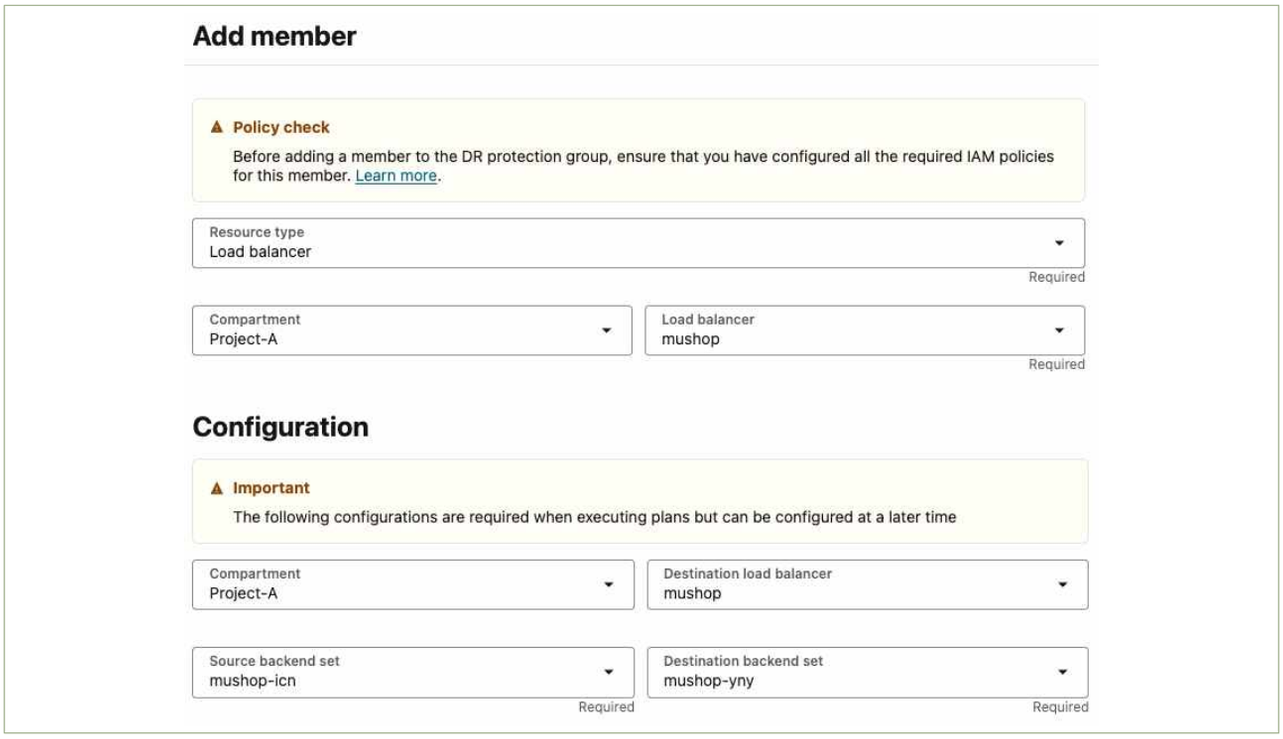




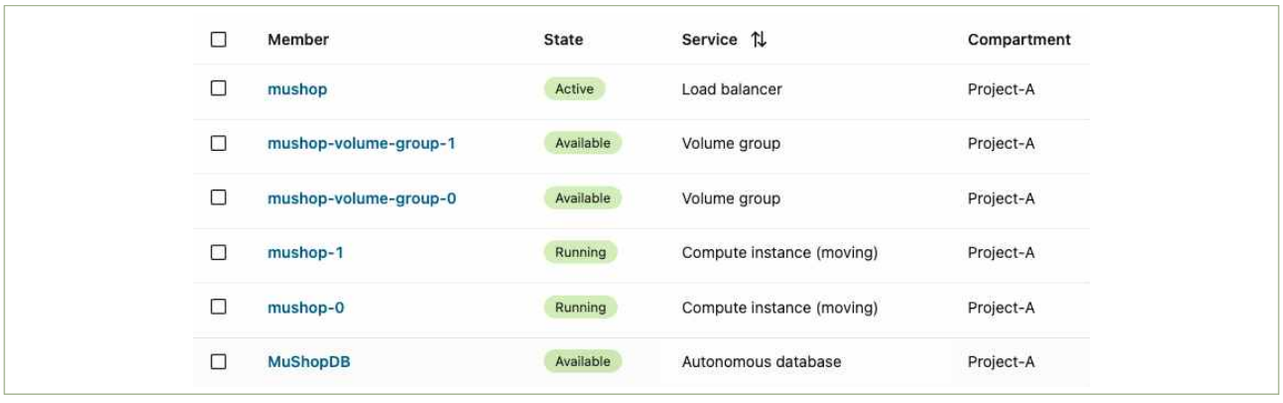
- Boot/Block Volume이 있는 Volume Group 추가(다수의 볼륨 그룹에 대해 동일한 방식으로 적용 가능)



- Load Balancer 추가

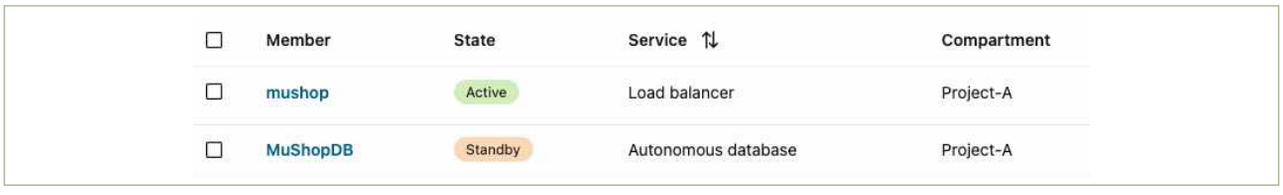


- Primary 리전의 DR protection group에 멤버 추가 완료 결과



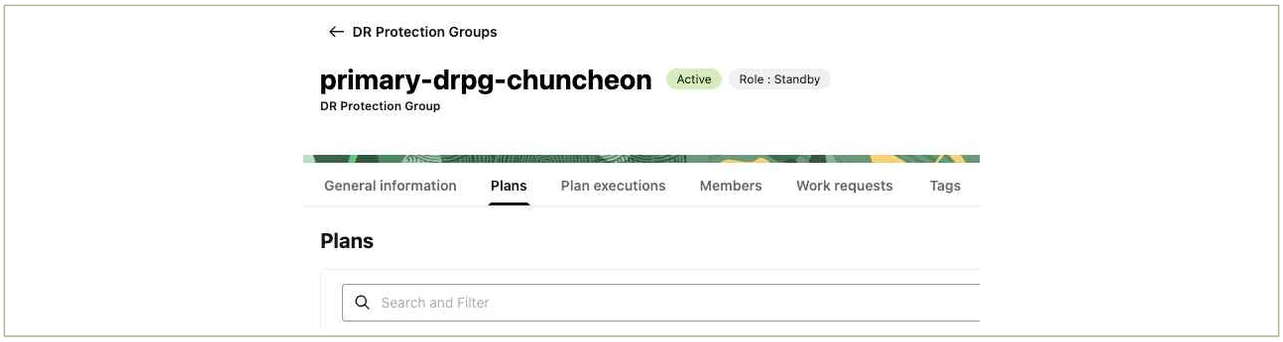
Member	State	Service	Compartment
mushop	Active	Load balancer	Project-A
mushop-volume-group-1	Available	Volume group	Project-A
mushop-volume-group-0	Available	Volume group	Project-A
mushop-1	Running	Compute instance (moving)	Project-A
mushop-0	Running	Compute instance (moving)	Project-A
MuShopDB	Available	Autonomous database	Project-A

- Standby 리전의 DR protection group에서 Members 탭을 클릭하여 멤버를 추가: Autonomous Database의 Standby와 Load Balancer만 추가

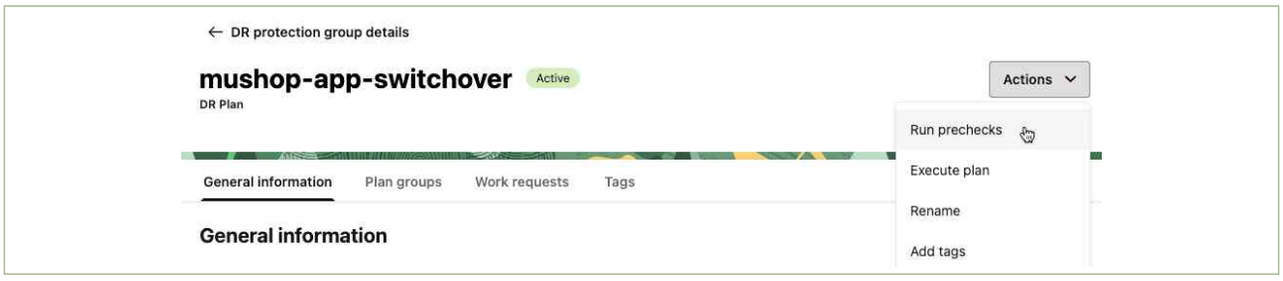


Member	State	Service	Compartment
mushop	Active	Load balancer	Project-A
MuShopDB	Standby	Autonomous database	Project-A

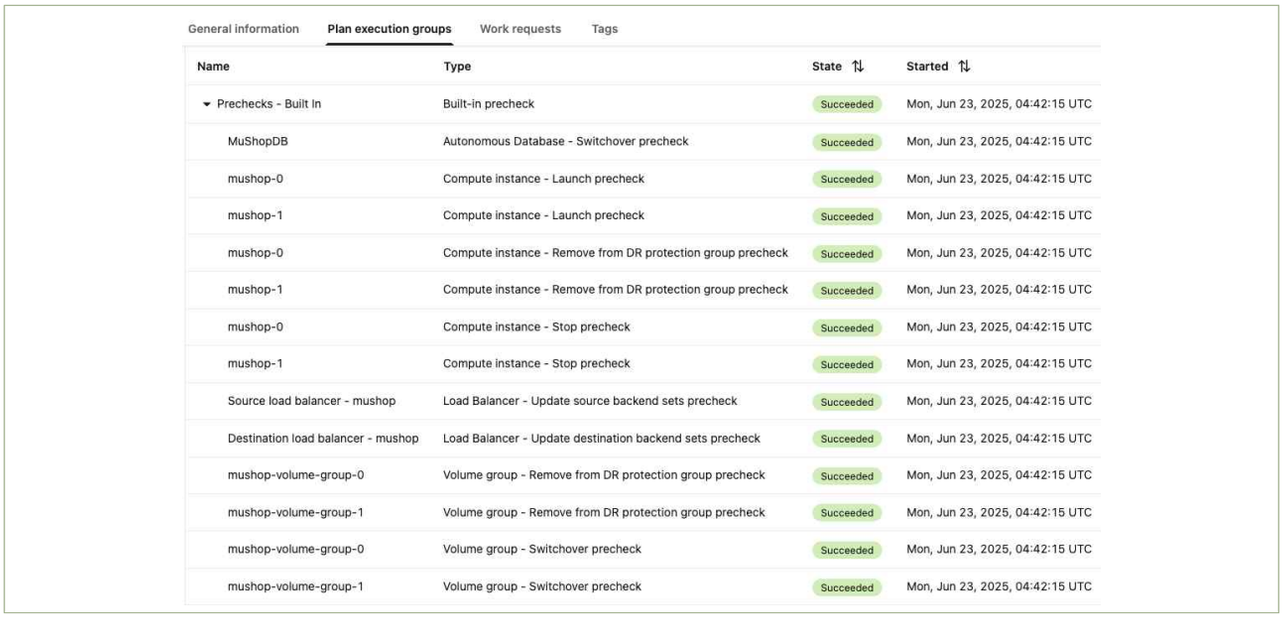
- StandBy 리전에서 DR Switchover Plan 생성
- Plans 탭에서 Create plan을 클릭: 테스트를 위해 Switchover 플랜 생성



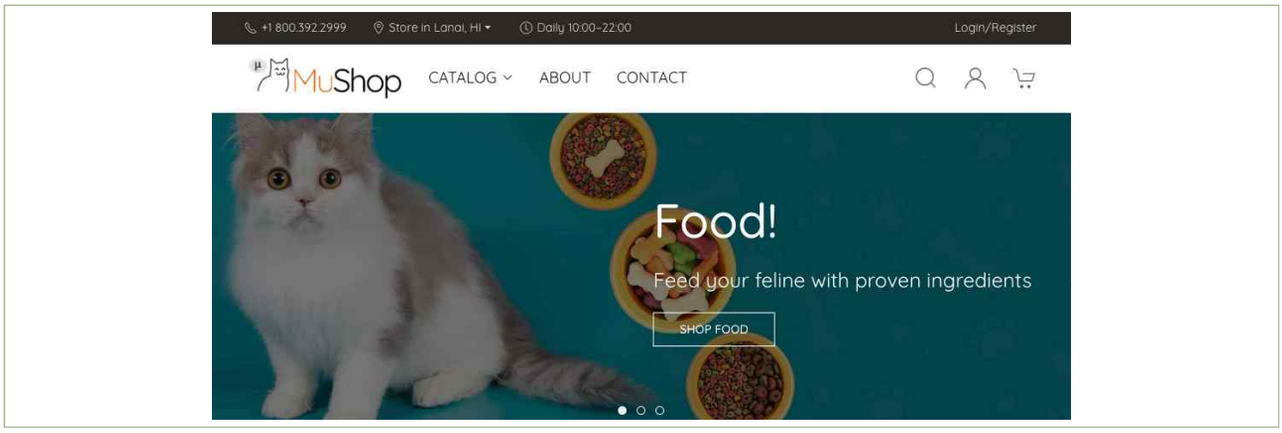
- 생성된 DR Plan으로 이동하여, 사전 체크를 위해 Run prechecks를 실행



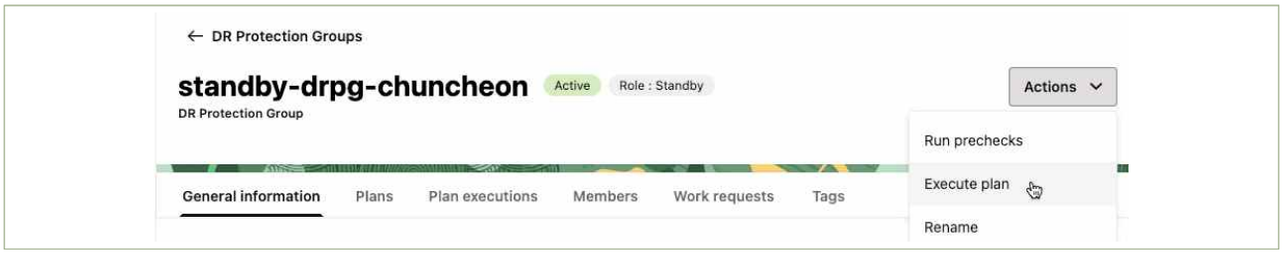
- Run prechecks의 결과 확인

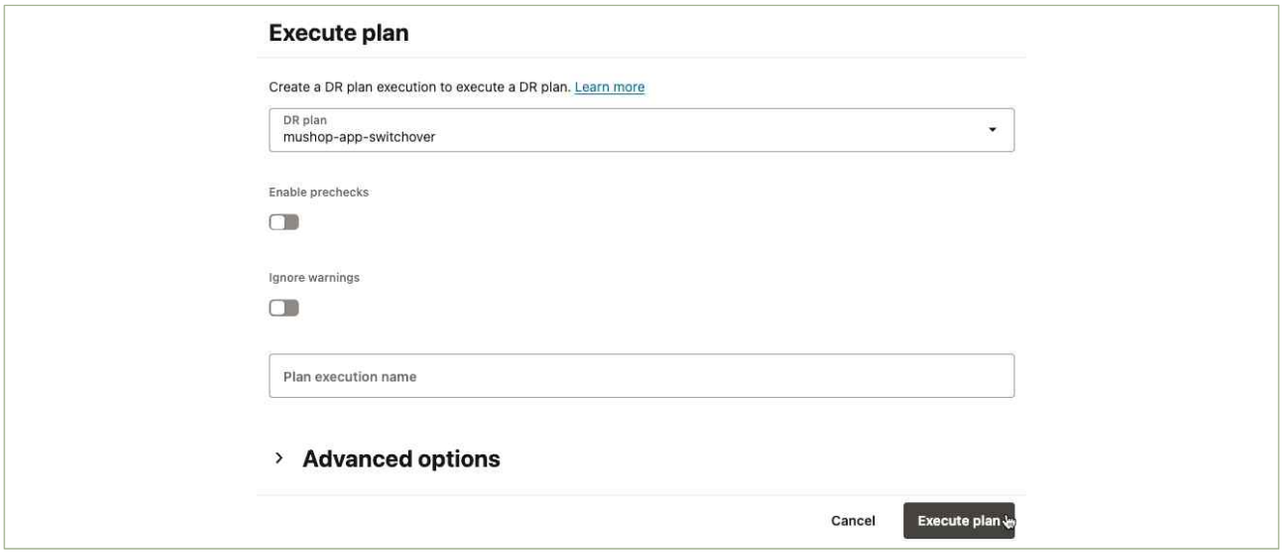


- Primary 리전에서 (OCI 콘솔) '홈' → 'Networking' → 'Load balancers' → 'Load balancer' → 현재 Primary 리전에 구성된 Load Balancer의 Public IP를 확인하여 웹 브라우저에서 접속 여부 확인

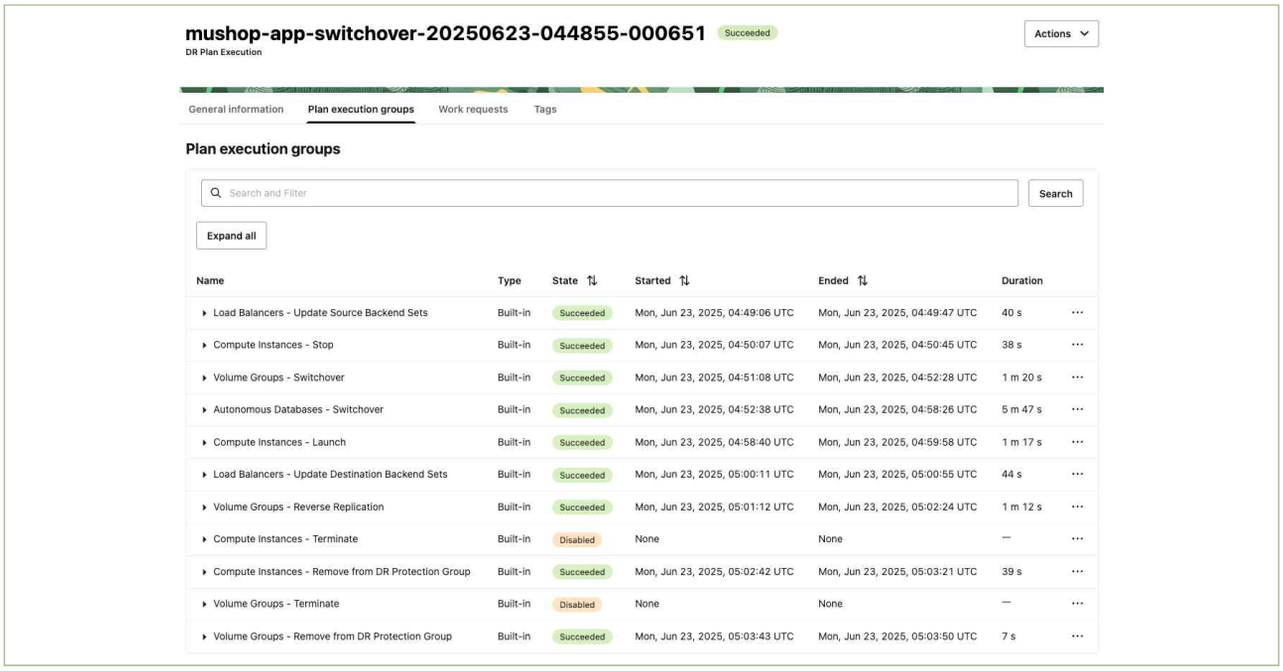


- Standby 리전에서 (OCI 콘솔) '홈' → 'Migration and Disaster Recovery' → 'Disaster Recovery' → 'DR Protection Groups'
- DR protection group의 Actions 메뉴에서 Execute plan을 클릭하여 Plan 실행





- 실행 결과 확인(실행 시간은 대상 애플리케이션과 환경 구성에 따라 상이함)



- Standby 리전에서, (OCI 콘솔) '홈' → 'Networking' → 'Load balancers' → 'Load balancer'로 이동하여, 현재 Standby리전에 failover된 Load Balancer의 Public IP를 확인하여 웹 브라우저에서 접속 여부 확인

4 참고 사항

- OCI High Availability, Disaster Recovery, and Reliability: A Complete Comparison
  https://www.ateam-oracle.com/post/oci-high-availability-disaster-recovery-and-reliability-a-complete-comparison
- OCI Technology Implementation - High Availability
  https://docs.public.content.oci.oraclecloud.com/en-us/iaas/Content/cloud-adoption-framework/high-availability.htm
- 한국정보통신기술협회(TTA)의 정보시스템 재해복구 지침
  https://cisp.or.kr/wp-content/uploads/2016/09/20160903_082806.pdf
- Oracle Cloud Accelerates Expansion to Bring Infrastructure to Customers Globally
  https://www.oracle.com/corporate/pressrelease/oow19-oracle-cloud-accelerates-global-expansion-091619.html

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 (ORACLE)

발 행 일	2025년 10월
발 행 인	금융보안원(원장 박상원)
공 동 발 행 인	ORACLE
금 융 보 안 원	
클라우드대응부	부장 김제광
클라우드기획팀	팀장 장지현 차장 정희선 과장 김용규 과장 안성현 과장 마승영 대리 최주섭 대리 송창석 주임 전동현 주임 전하은
발 행 처	금융보안원
	02-3495-9000
	경기도 용인시 수지구 대지로 132

〈비 매 품〉

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서