SK 쉴더스

2023 클라우드 보안 가이드

- Azure

2023 클라우드 보안 가이드 발간사

안녕하십니까? SK쉴더스입니다.

지난 21년 SK쉴더스의 취약점진단팀은 "클라우드 보안 가이드 - AWS, Azure, GCP" 3종을 발간했습니다.

현재 On-Premise 환경에서 클라우드 환경으로 전환하거나, 하이브리드 형태로 전환하고 있는 기업들이 늘어나고 있으며, CSP(클라우드 서비스 제공업체) 별 네이티브 서비스와 관리 영역의 많은 변화로 인해 보안정책 설정 및 환경설정을 대응하고자 클라우드 운영자 및 관리자는 많은 어려움을 겪고 있습니다.

특히, 최근 AWS, Azure의 관리 영역 및 네이티브 서비스의 변화가 많았습니다.
이러한 트렌드를 분석하고 변화에 대응하고자 올해도 "2023 클라우드 보안 가이드 - AWS, Azure, GCP" 3종의 개정판을 발간하게 되었습니다.

이번 가이드는 ISMS 인증심사(기술영역)을 대응하고자 항목분류를 개편하였으며, 클라우드 운영자가 위협에 대응하고 변화된 관리 영역 및 컴플라이언스 기준을 충족할 수 있는 기준을 제시했습니다.

앞으로도 SK쉴더스는 클라우드 운영자와 더불어 관리자도 다양한 환경에 발빠르게 대응할 수 있도록 보안 가이드를 개선하여 발간할 계획입니다.

더불어, 1년 동안 클라우드 보안가이드 개선에 많은 시간과 노력을 투자해준 팀원들에게 감사의 인사를 드립니다.

감사합니다.

ICT사업그룹 취약점진단팀 팀장
김 상 춘

목 차

I. 전체목록

1. 체크리스트 항목

진단에 사용될 체크리스트는 국내·외 공식 기술 자료를 바탕으로 작성 되었습니다. Azure 보안가이드에서의 영역은 계정 관리(9개 항목), 권한 관리(6개 항목), 가상 리소스 관리(9개 항목), 운영 관리(11개 항목)으로 총 4개 영역에서 35개 항목으로 구성 하였습니다.

[표] 1. Azure 보안진단 체크리스트

영역	항목코드	항목명	중요도
계정 관리	1.1	AD 사용자 계정 관리	상
	1.2	AD 사용자 프로필 및 디렉터리 식별 관리	중
	1.3	AD 그룹 소유자 및 구성원 관리	중
	1.4	AD 게스트 사용자	상
	1.5	AD 암호 재설정 규칙 관리	하
	1.6	SSH Key 접근 관리	하
	1.7	MFA (Multi-Factor-Authentication) 설정	상
	1.8	MFA 계정 잠금 정책 관리	중
	1.9	Azure 패스워드 정책 관리	중
권한 관리	2.1	구독 액세스 제어(IAM) 역할 관리	상
	2.2	리소스 그룹 액세스 제어(IAM) 역할 할당	상
	2.3	AD 사용자 역할 권한 관리	상
	2.4	인스턴스 서비스 액세스 정책 관리	상
	2.5	네트워크 서비스 액세스 정책 관리	상
	2.6	기타 서비스 액세스 정책 관리	상
가상 리소스 관리	3.1	가상 네트워크 리소스 관리	중
	3.2	내부 가상 네트워크 보안 관리	상
	3.3	보안그룹 인/아웃바운드 ANY 설정 관리	상
	3.4	보안그룹 인/아웃바운드 불필요 정책 관리	중
	3.5	방화벽 ANY 정책 설정 관리	상
	3.6	방화벽 불필요 정책 관리	중
	3.7	NAT 게이트웨이 서브넷 연결 관리	중
	3.8	스토리지 계정 보안 설정	상
	3.9	스토리지 계정 공유 액세스 서명 정책 관리	중
운영 관리	4.1	데이터베이스 암호화 설정 관리	중
	4.2	스토리지 암호화 설정	상
	4.3	디스크 암호화 설정	상
	4.4	통신구간 암호화 설정	중
	4.5	키 자격 증명 모음 회전 정책 관리	중
	4.6	AD 감사로그 설정	상

	4.7	인스턴스 서비스 감사 로그 설정	중
	4.8	네트워크 서비스 감사 로그 설정	중
	4.9	기타 서비스 감사 로그 설정	중
	4.10	리소스 그룹 잠금	하
	4.11	백업 사용 여부	중

2. Azure 보안가이드/ISMS 매칭 기준 항목

ISMS-P 영역의 "2. 보호대책 요구사항" 전체 64개 항목 중 31개 항목을 매핑(48%)하였습니다. 전체 항목 중 일부 영역 항목인 "정책 및 조직 관리", "보안 서약 및 교육 훈련", "물리 보안", "사고 예방 및 취약점 점검 조치" 등과 같은 클라우드 환경에서의 직접 확인 및 증적 마련이 불가능한 항목은 28개입니다. 이와 같은 항목은 회사 내규 및 자체적으로 관리되고 있는 문서로 증적을 대체하여야 합니다.

[표] 2. Azure 보안가이드와 ISMS 항목 매칭

영역	항목 코드	항목명	ISMS 기준항목
계정 관리	1.1	AD 사용자 계정 관리	2.2.1 주요 직무자 지정 및 관리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리
	1.2	AD 사용자 프로필 및 디렉터리 식별 관리	2.1.3 정보자산 관리 2.5.1 사용자 계정 관리 2.5.2 사용자 식별
	1.3	AD 그룹 소유자 및 구성원 관리	2.5.1 사용자 계정 관리
	1.4	AD 게스트 사용자	2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리
	1.5	AD 암호 재설정 규칙 관리	2.7.1 암호정책 적용
	1.6	SSH Key 접근 관리	2.6.2 정보시스템 접근 2.6.6 원격접근 통제
	1.7	MFA (Multi-Factor-Authentication) 설정	2.5.3 사용자 인증 2.5.4 비밀번호 관리 2.6.2 정보시스템 접근 2.6.6 원격접근 통제
	1.8	MFA 계정 잠금 정책 관리	2.7.1 암호정책 적용
	1.9	Azure 패스워드 정책 관리	2.5.4 비밀번호 관리
권한 관리	2.1	구독 액세스 제어(IAM) 역할 관리	2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근
	2.2	리소스 그룹 액세스 제어(IAM) 역할 할당	2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리

			2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근
	2.3	AD 사용자 역할 권한 관리	2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근
	2.4	인스턴스 서비스 액세스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근 2.6.4 데이터베이스 접근 2.10.2 클라우드 보안
	2.5	네트워크 서비스 액세스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근 2.10.2 클라우드 보안
	2.6	기타 서비스 액세스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근 2.6.3 응용프로그램 접근 2.8.5 소스 프로그램 관리 2.10.2 클라우드 보안
가상 리소스 관리	3.1	가상 네트워크 리소스 관리	2.6.7 인터넷 접속 통제
	3.2	내부 가상 네트워크 보안 관리	2.6.1 네트워크 접근
	3.3	보안그룹 인/아웃바운드 ANY 설정 관리	2.6.1 네트워크 접근 2.6.6 원격접근 통제
	3.4	보안그룹 인/아웃바운드 불필요 정책 관리	2.6.1 네트워크 접근

	3.5	방화벽 ANY 정책 설정 관리	2.6.1 네트워크 접근 2.6.6 원격접근 통제
	3.6	방화벽 불필요 정책 관리	2.6.1 네트워크 접근 2.6.6 원격접근 통제 2.8.3 시험과 운영 환경 분리
	3.7	NAT 게이트웨이 서브넷 연결 관리	2.6.1 네트워크 접근
	3.8	스토리지 계정 보안 설정	2.6.1 네트워크 접근 2.6.2 정보시스템 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제 2.10.3 공개서버 보안
	3.9	스토리지 계정 공유 액세스 서명 정책 관리	2.6.1 네트워크 접근 2.6.2 정보시스템 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제 2.10.3 공개서버 보안
운영 관리	4.1	데이터베이스 암호화 설정 관리	2.7.1 암호정책 적용
	4.2	스토리지 암호화 설정	2.7.1 암호정책 적용
	4.3	디스크 암호화 설정	2.7.1 암호정책 적용
	4.4	통신구간 암호화 설정	2.7.1 암호정책 적용 2.10.5 정보전송 보안
	4.5	키 자격 증명 모음 회전 정책 관리	2.7.2 암호키 관리
	4.6	AD 감사로그 설정	2.5.6 접근권한 검토 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.7	인스턴스 서비스 감사 로그 설정	2.5.6 접근권한 검토 2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.8	네트워크 서비스 감사 로그 설정	2.5.6 접근권한 검토 2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및

			모니터링
	4.9	기타 서비스 감사 로그 설정	2.5.6 접근권한 검토 2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.10	리소스 그룹 잠금	2.9.1 변경관리
	4.11	백업 사용 여부	2.9.2 성능 및 장애관리 2.9.3 백업 및 복구 관리 2.12.2 재해 복구 시험 및 개선

3. 위험도 구분

각 취약점으로 인해 발생 가능한 피해에 대하여 위험도 산정을 통해 상, 중, 하 3단계로 분류함.

[표] 2. 위험도 구분

위험도	내 용	조치기간	비고
상	관리자 계정 및 주요정보 유출로 인한 치명적인 피해 발생	단기	
중	노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생 우려	중기	
하	타 취약점과 연계 가능한 잠재적인 위협 내재	장기	

2. 세부항목 설정

1. 계정 관리

1.1 AD 사용자 계정 관리

<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">AD 사용자 계정 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
Azure AD(Azure Active Directory)는 클라우드 기반 ID 및 액세스 관리 서비스입니다. 이 서비스를 통해 Microsoft 365, Azure Portal 및 수천 개의 기타 SaaS 애플리케이션과 같은 외부 리소스에 액세스할 수 있습니다. 또한 Azure Active Directory는 조직용으로 개발된 클라우드 앱과 함께 회사 인트라넷 네트워크의 앱과 같은 내부 리소스에 액세스할 수 있도록 도와줍니다.

Azure AD를 사용하는 사용자의 효율적인 관리를 위해 프로필을 구성할 수 있으며, 네이밍룰 등을 적용하여 사용자의 권한, 역할 등을 표기하여 관리할 수 있습니다. 또한 디렉터리 역할 설정을 통해 사용자의 관리 역할 부여가 가능합니다.

Azure에서 호스트되는 서비스의 경우 가능한 경우 관리 ID를 사용하고 그렇지 않은 경우 서비스 주체를 사용하는 것이 좋습니다. 관리 ID는 Azure 외부에서 호스팅 되는 서비스에 사용할 수 없습니다. 이 경우 서비스 주체를 권장합니다. 관리 ID 또는 서비스 주체를 사용할 수 있는 경우 이 작업을 수행합니다.

※ 사용자 생성 기본 디렉터리 역할
<table>
<tr><th>디렉터리 역할</th><th>내용</th></tr>
<tr><td>사용자</td><td>할당된 리소스에 액세스 할 수 있지만, 대부분의 디렉터리 리소스를 관리할 수 없음</td></tr>
<tr><td>전역 관리자</td><td>Azure AD의 전체 디렉터리 리소스에 대한 모든 권한을 보유</td></tr>
<tr><td>제한된 관리자</td><td>Azure AD의 복수개의 관리 역할을 보유</td></tr>
</table>

※ 사용자 계정 구분
<table>
<tr><th>계정 구분</th><th>내용</th></tr>
<tr><td>관리ID</td><td>개발자는 다양한 서비스 간의 통신을 보호하는 데 사용되는 암호 및 자격 증명을 관리하는 경우가 많습니다. 관리 ID는 Azure 리소스에 ID를 제공하기 위해 만든 보안 Azure AD(Azure Active Directory) ID입니다.</td></tr>
<tr><td>서비스 사용자</td><td>서비스 주체는 단일 Azure AD 테넌트에 있는 애플리케이션 개체의 로컬 표현입니다. 애플리케이션 인스턴스의 ID 역할을 하며, 애플리케이션에 액세스할 수 있는 사용자와 애플리케이션이 액세스할 수 있는 리소스를 정의합니다.</td></tr>
</table>
</td></tr>
</table>

Azure AD 서비스 계정	온-프레미스 사용자 계정에는 다른 Active Directory 사용자 계정과 마찬가지로 수동 암호 관리가 필요합니다. 서비스 및 도메인 관리자는 해당 계정을 안전하게 유지하기 위해 강력한 암호 관리 프로세스를 준수해야 합니다.

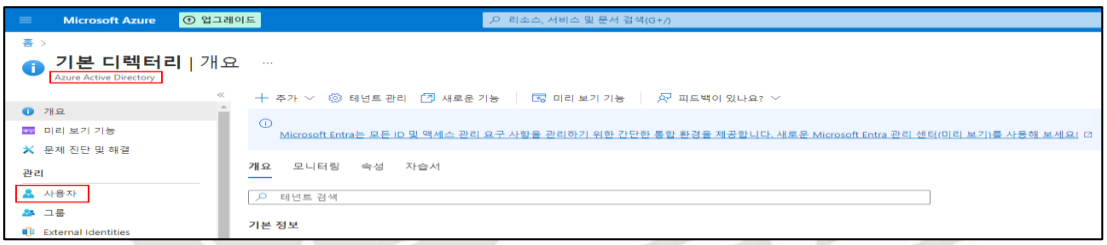
※ 불필요한 계정 예시

1. 비임직원 계정 (협력사 공통 계정)
2. 테스트 계정 (testuser, test01, test02....)
3. 미사용 계정 (퇴직 및 휴직자)

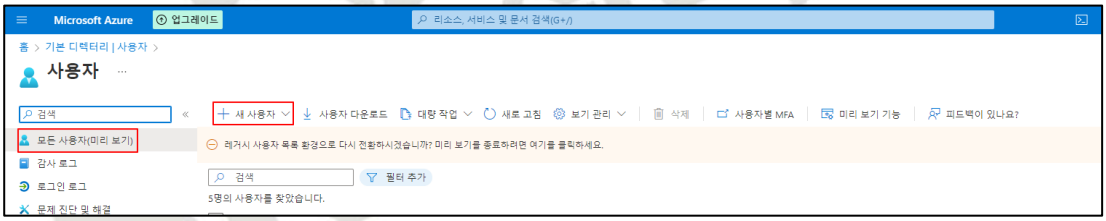
설정 방법

가. 전역/제한된 관리자 생성 및 설정 방법

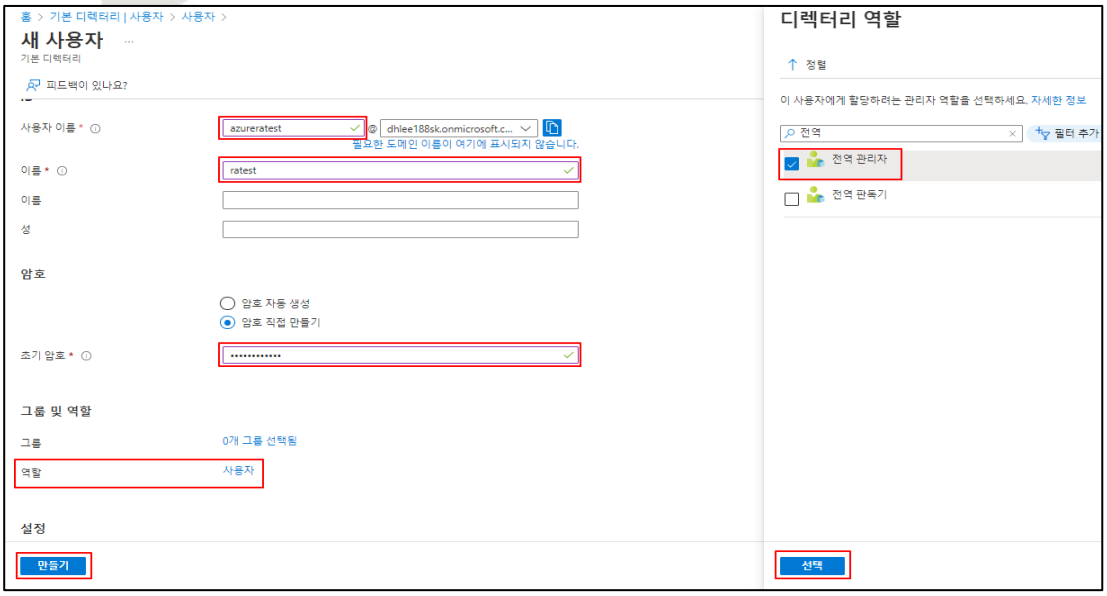
1) Azure Active Directory 메뉴 내 사용자 기능 선택

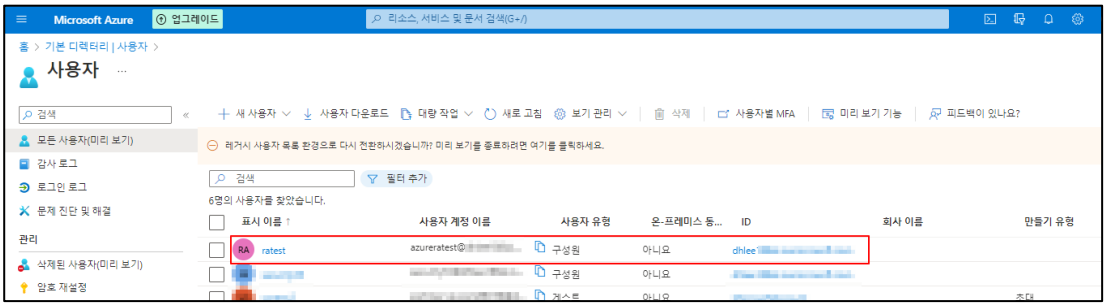
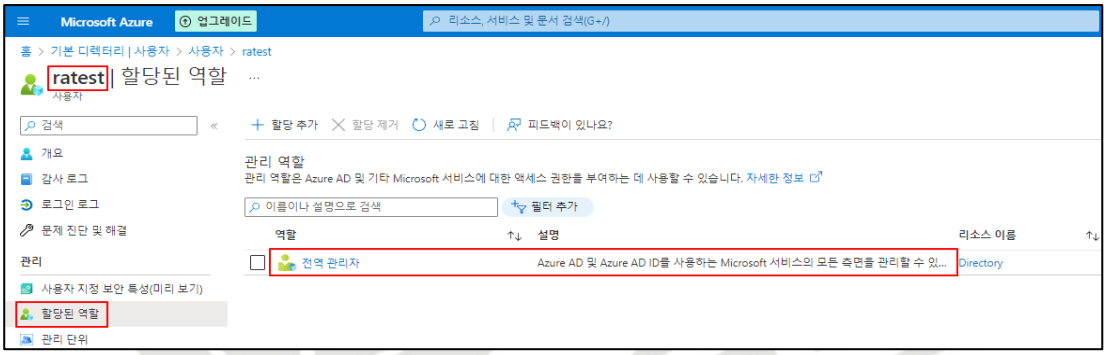


2) 모든 사용자 메뉴 내 새 사용자 버튼 클릭



3) 사용자 정보 입력 및 디렉터리 역할 선택 시 전역/제한된 관리자 선택



	4) 모든 사용자 목록 내 전역/제한된 관리자 생성 여부 확인  5) 모든 사용자 부여된 역할 확인 
진단 기준	**양호기준** : 전역관리자 권한을 보유한 다수 계정이 존재하지 않고 불필요한 계정이 존재하지 않을 경우 **취약기준** : 전역관리자 권한을 보유한 다수 계정 또는 불필요한 계정이 존재하는 경우
비고	

1.2 AD 사용자 프로필 및 디렉터리 식별 관리

분류	계정 관리	중요도	중
항목명	AD 사용자 프로필 및 디렉터리 식별 관리		
항목 설명	생성된 Active Directory 사용자에 대한 정보를 프로필 가능을 통해 추가, 수정할 수 있습니다. 사용자 계정에 대한 프로필 정보는 서비스 사용에 대한 식별/감사/추적 등을 명확하게 할 수 있기 때문에 정확한 정보를 기입하는 것이 필요합니다. **※ 프로필 작성 필수 항목** ID - 계정 사용자 성명 기입 작업 정보 - 부서/직함 기입, 관리자 선택 (게스트 계정일 경우 필수) 연락처 정보 - 메일 주소 기입		
설정 방법	**가. 사용자 프로필 정보 확인 및 설정 방법** 1) Active Directory의 사용자 리스트 내 개별 사용자 클릭  2) 사용자 메뉴의 속성 편집 버튼 클릭  		

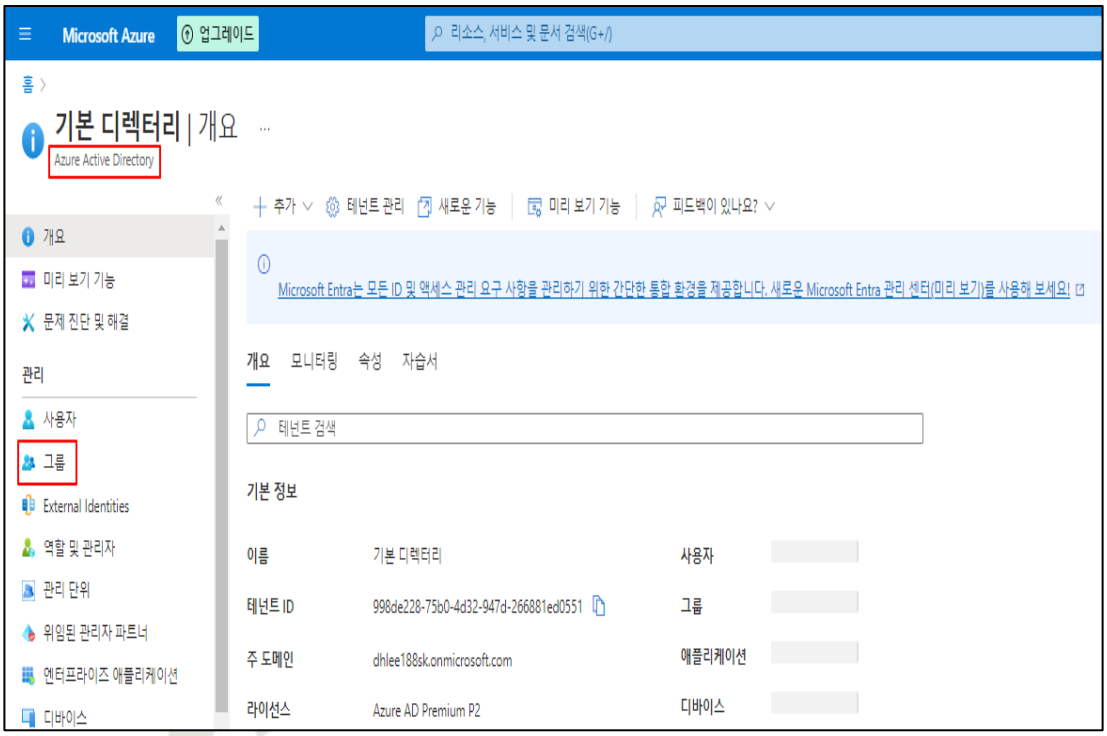
3) 속성 정보 확인 및 수정(ID)

4) 속성 정보 수정(연락처)

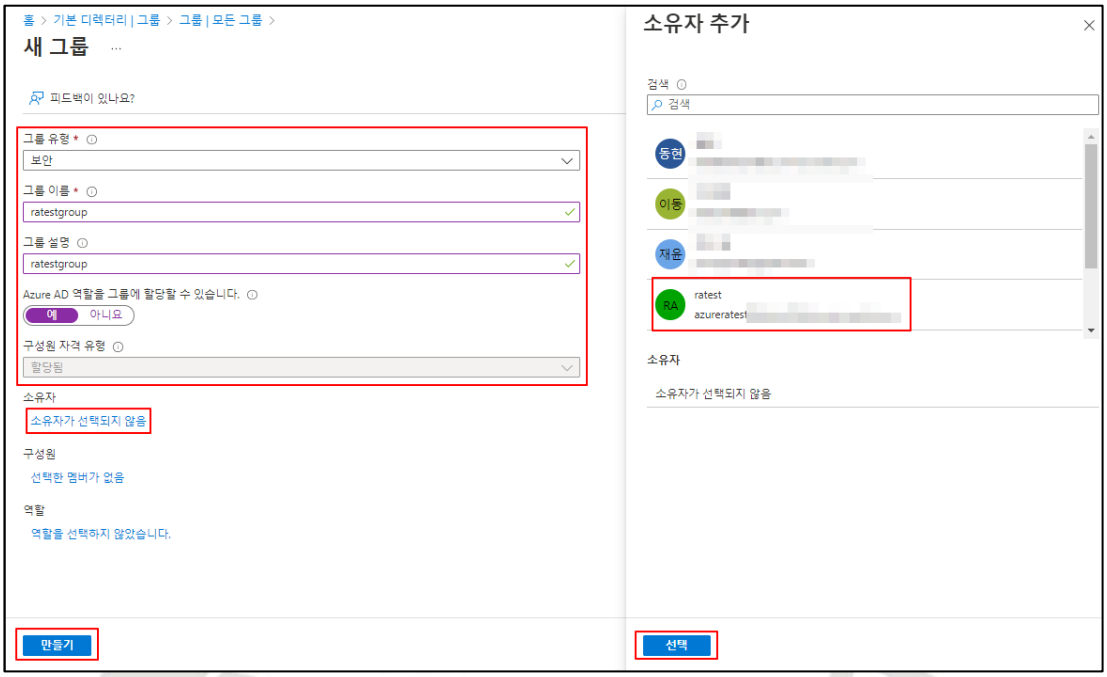
5) 속성 정보 수정(작업 정보) 후 저장 클릭

진단 기준	**양호기준** : 프로필 필수 항목(ID, 작업정보, 연락처 등)이 작성되어 있을 경우 **취약기준** : 프로필 필수 항목(ID, 작업정보, 연락처 등)이 작성되어 있지 않을 경우
비고	

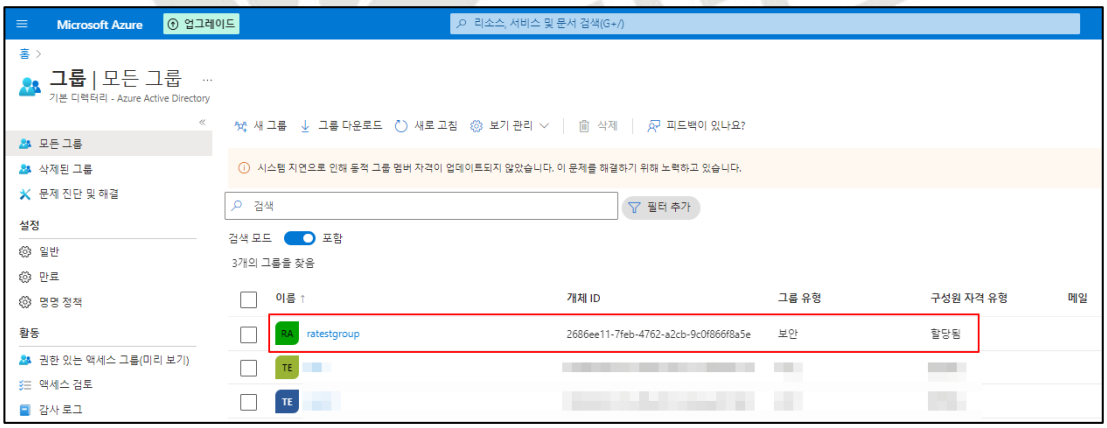
1.3 AD 그룹 소유자 및 구성원 관리

분류	계정 관리	중요도	중
항목명	AD 그룹 소유자 및 구성원 관리		
항목 설명	Azure AD를 사용 시 그룹을 통해 권한을 할당하거나 리소스에 대한 액세스 권한을 부여할 수 있으며, 해당 그룹 구성원인 사용자는 그룹의 액세스 권한을 상속받게 됩니다. 또한 그룹은 소유자를 지정하여 그룹 및 그룹 구성원을 관리할 수 있습니다.		
설정 방법	**가. Azure Active Directory(Azure AD) 그룹 생성 및 소유자 설정 방법** 1) Azure AD 메뉴 내 그룹 기능 선택  2) 그룹메뉴 내 새 그룹 버튼 클릭 		

3) 그룹 관련 내용 설정 및 만들기(소유자 추가 설정 필요)

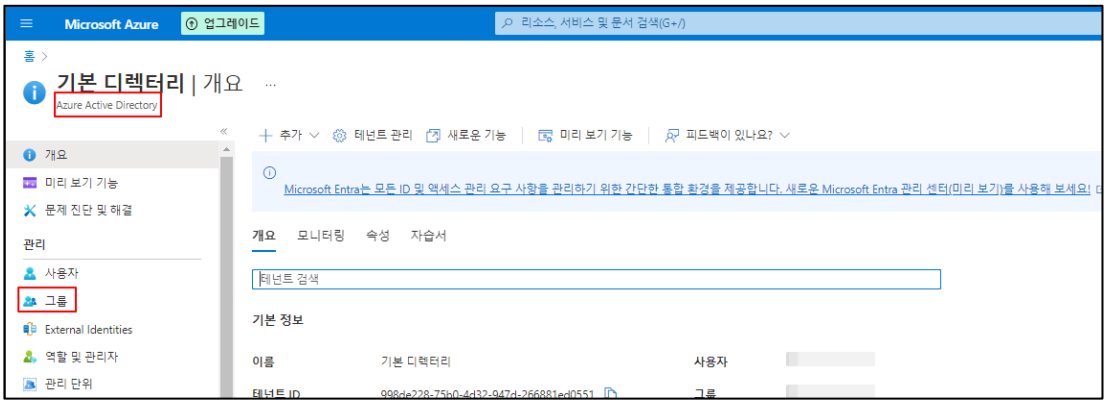


4) 모든 그룹 목록 내 정상 생성 여부 확인



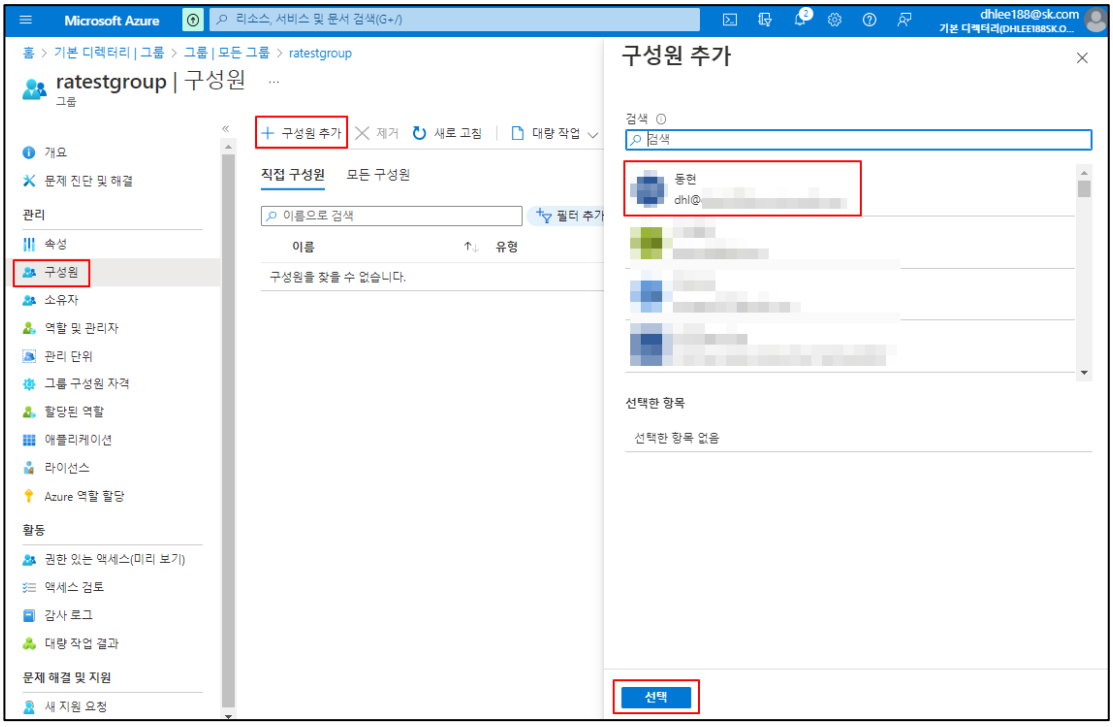
나. Azure Active Directory(Azure AD) 그룹 내 역할별 구성원 설정 방법

1) Azure AD 메뉴 내 그룹 기능 선택

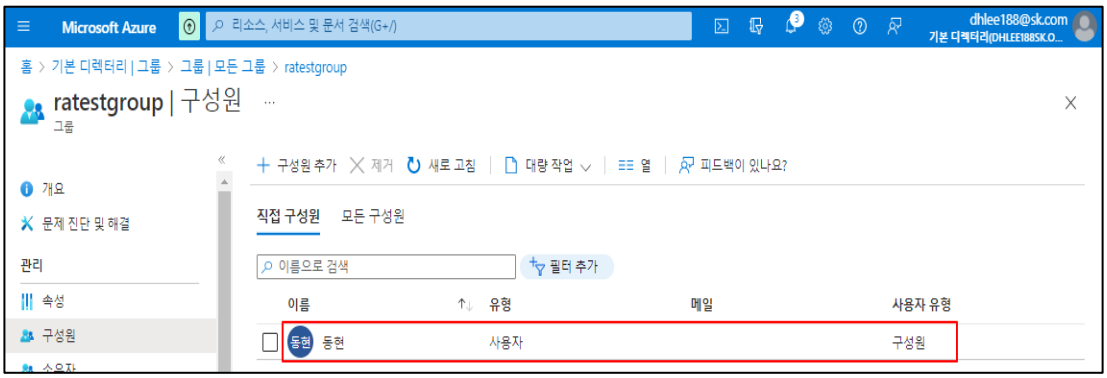


2) 소유자/구성원을 추가할 그룹 선택

3) 구성원 기능 선택 후 구성원 추가 버튼 클릭 및 추가할 구성원 검색(소유자 설정 방식 동일)

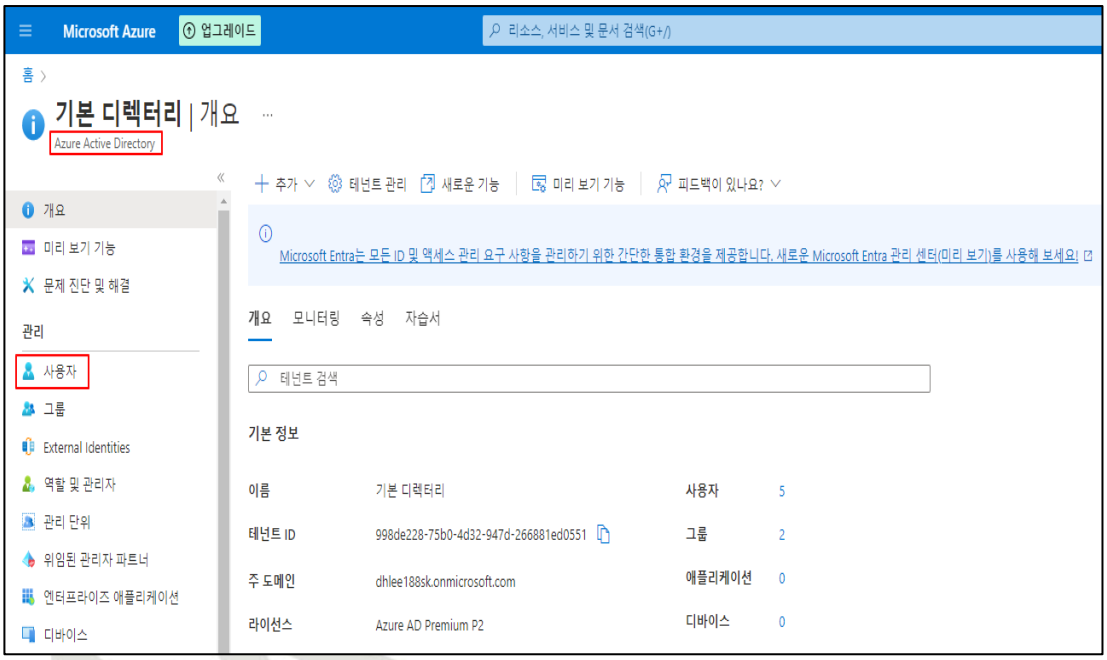
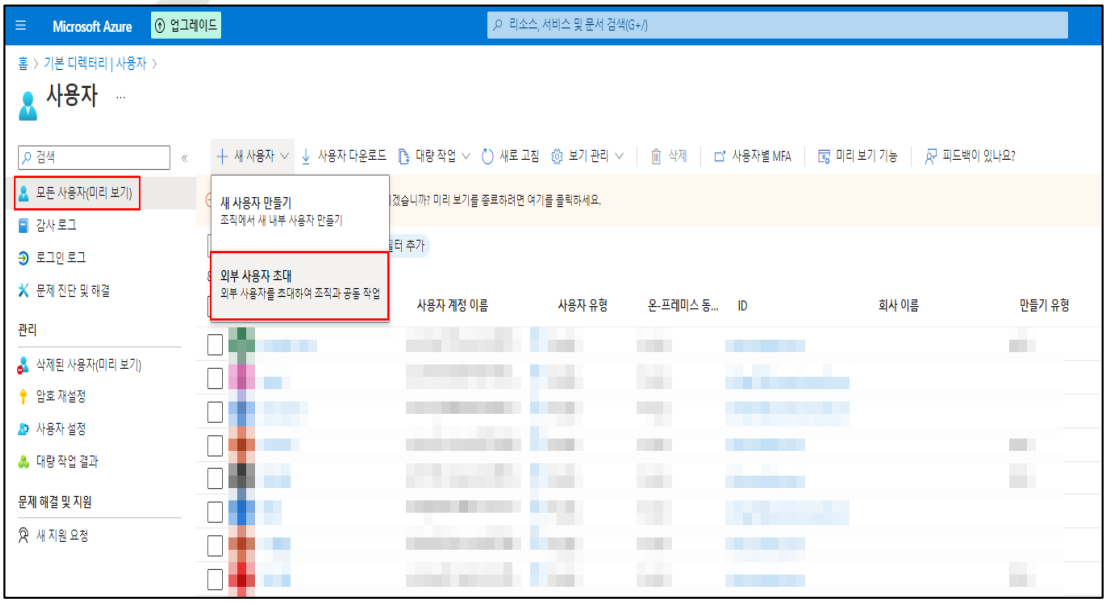


4) 구성원 목록 내 정상 생성 여부 확인

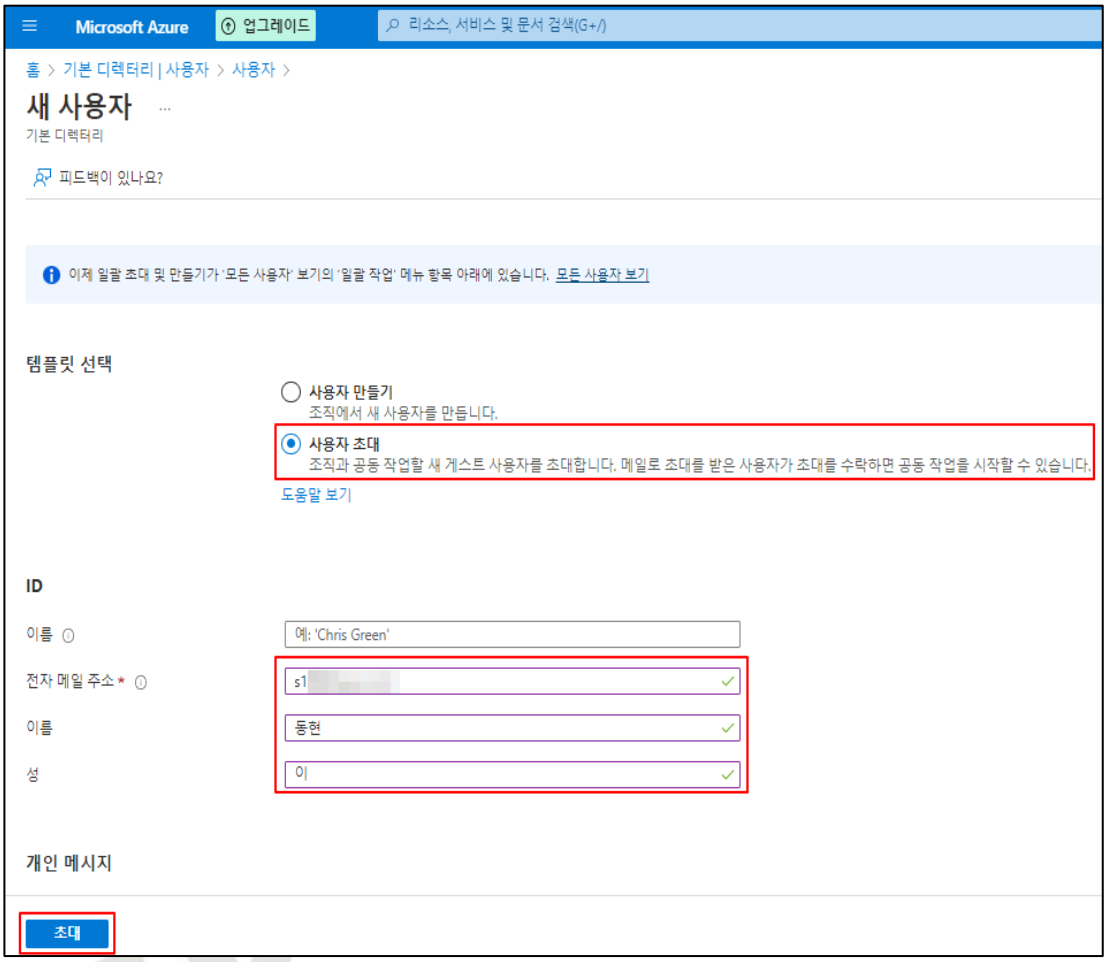


진단 기준	**양호기준** : 그룹에 소유자 및 구성원이 설정되어 있을 경우 **취약기준** : 그룹에 소유자 및 구성원이 설정되어 있지 않을 경우
비고	

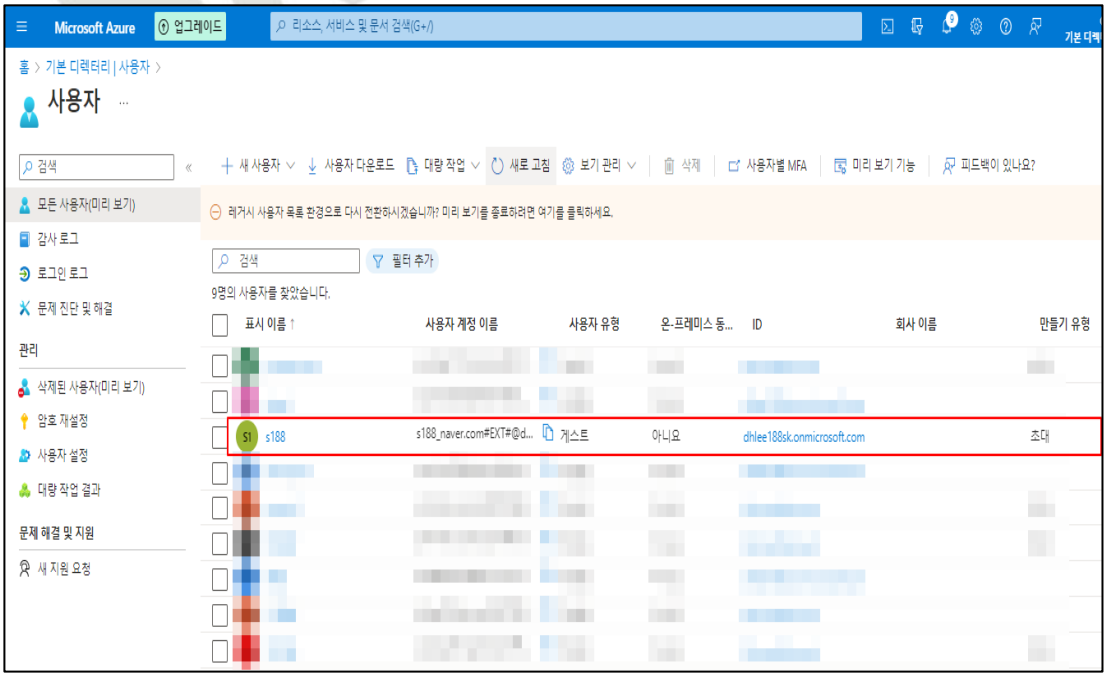
1.4 AD 게스트 사용자

분류	계정 관리	중요도	상
항목명	AD 게스트 사용자		
항목 설명	조직과 공동 작업하는 모든 사용자를 Azure AD(Active Directory)의 게스트 사용자로 추가하여 초대할 수 있습니다. 게스트 사용자는 기본적으로 제한적인 권한을 갖고 있지만, 기본 제한을 해제하여 AD 게스트 사용자에게 구성원 사용자와 동일한 권한을 부여할 수 있습니다.		
설정 방법	**가. 게스트 사용자 설정 방법** 1) Azure Active Directory 메뉴 내 사용자 기능 선택  2) 모든 사용자 메뉴 내 외부 사용자 초대 클릭 		

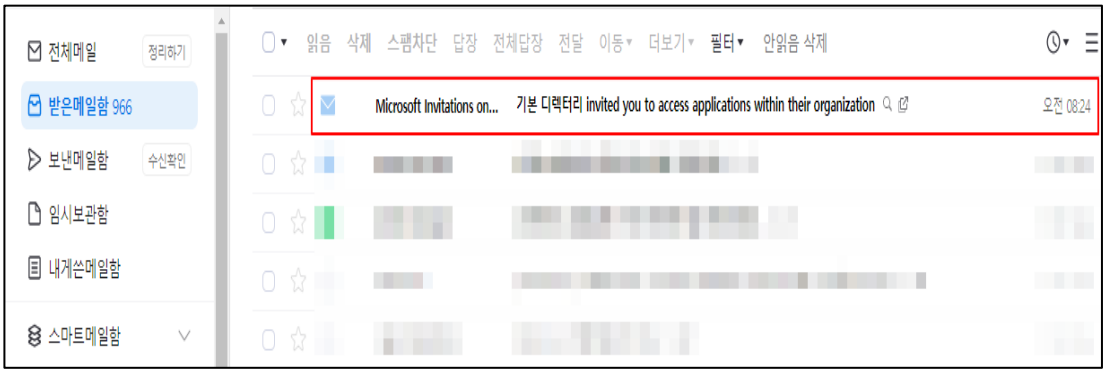
3) 초대할 게스트 사용자의 E-mail 주소 입력 및 초대



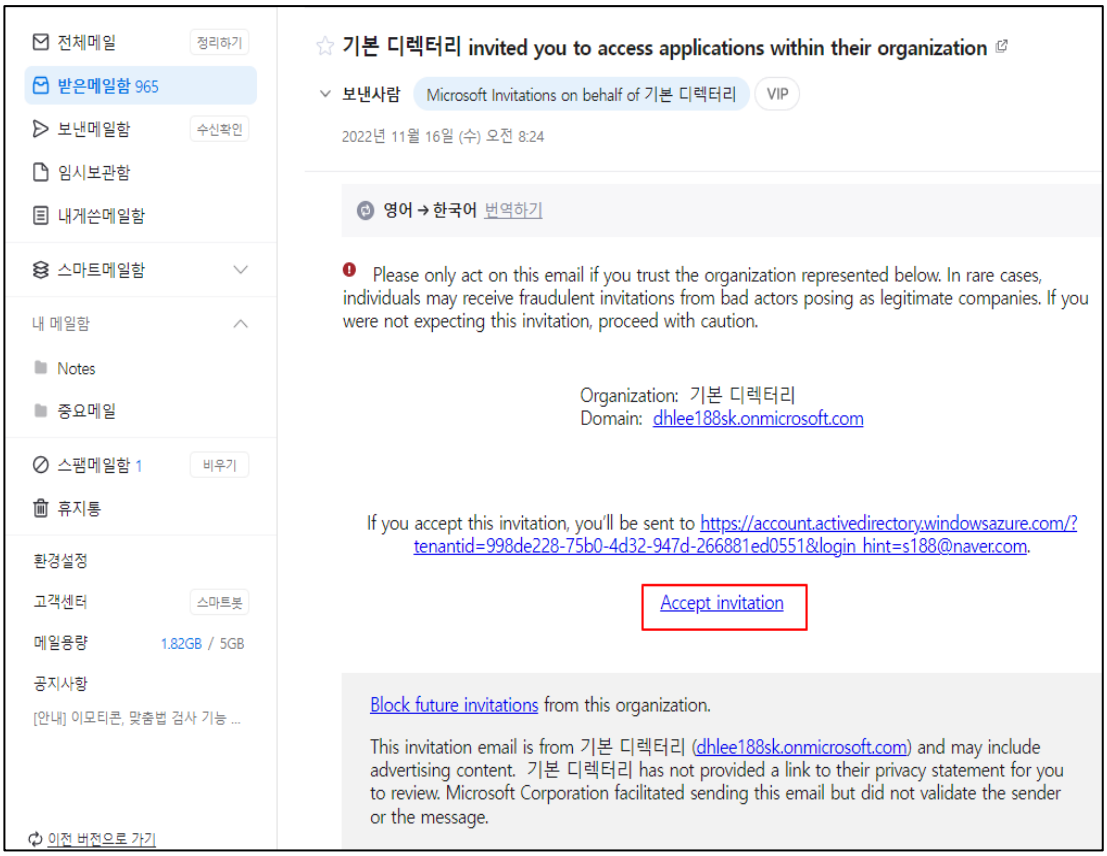
4) 모든 사용자 목록 내 게스트 사용자 초대 정상 여부 확인



5) 게스트 사용자 초대 메일 수신 (초대받은 게스트 사용자 시점)



6) 메일 내용 내 시작 버튼 클릭



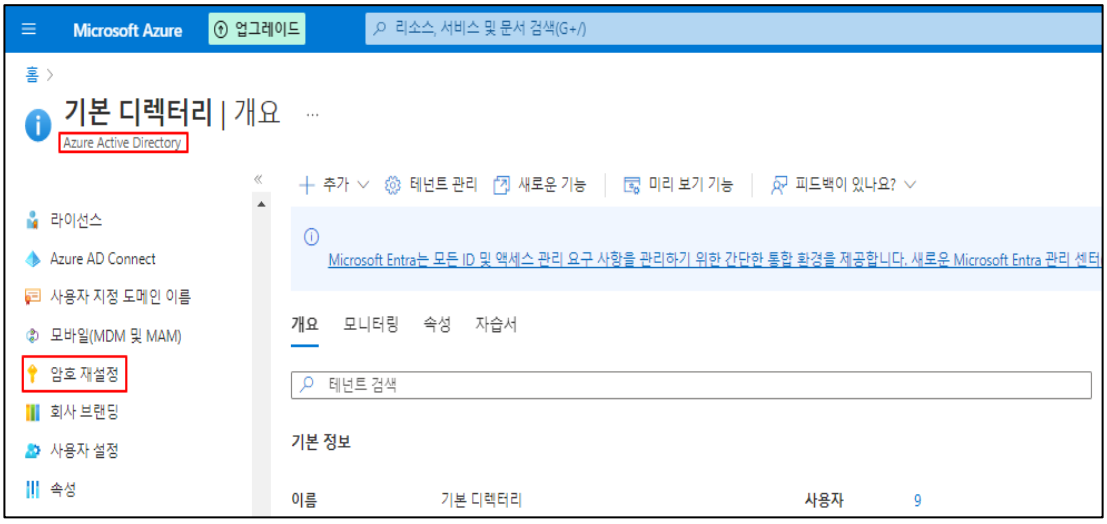
7) Azure 정상 로그인 여부 확인

진단 기준	**양호기준** : 게스트 사용자 계정(사용 만료 된 불필요한 계정 포함)을 사용하지 않을 경우 **취약기준** : 게스트 사용자 계정(사용 만료 된 불필요한 계정 포함)을 사용하고 있을 경우
비고	

1.5 AD 암호 재설정 규칙 관리

<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>하</td></tr>
<tr><td>항목명</td><td colspan="3">AD 암호 재설정 규칙 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure AD(Active Directory) 셀프 서비스 암호 재설정은 사용자가 자신의 암호를 재설정할 수 있도록 웹 기반 및 Windows 통합 환경을 제공합니다. 이를 통해 사용자는 모든 디바이스에서 언제 어디서나 암호를 관리할 수 있습니다. 다만, 사용자가 사용할 수 있는 인증 방법 유형을 변경하면 사용 가능한 최소 데이터 양이 없는 경우 사용자가 실수로 SSPR을 사용할 수 없게 될 수 있습니다. (*) SSPR: Self Service Password Reset

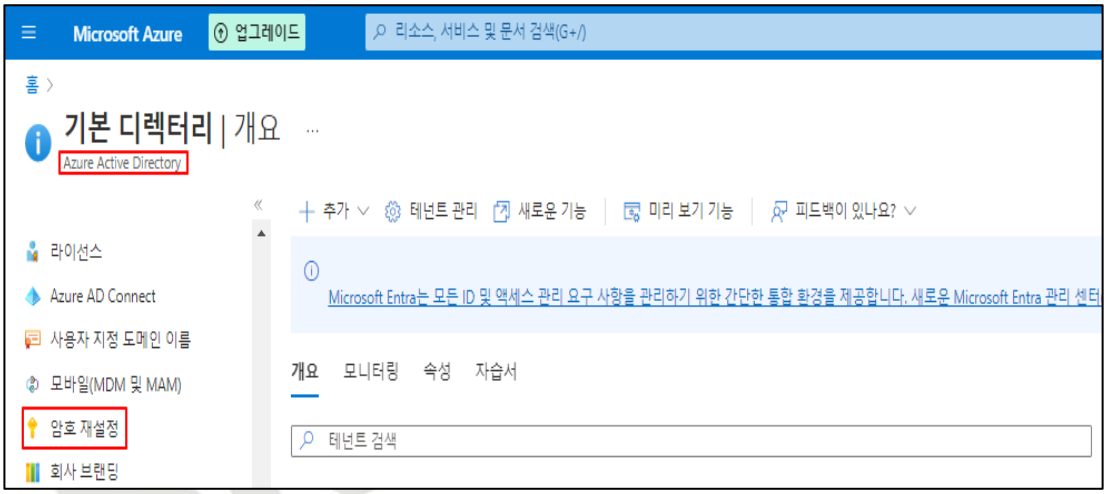
※ 암호 재설정 인증 방식
<table>
<tr><th>구분</th><th>내용</th></tr>
<tr><td>모바일 앱 알림</td><td>모바일 OTP 앱에서의 접근 허용 방식</td></tr>
<tr><td>모바일 앱 코드</td><td>모바일 OTP 앱에서의 코드 발생 후 접근 허용 방식</td></tr>
<tr><td>E-Mail</td><td>E-Mail 발송을 통한 접근 허용 방식</td></tr>
<tr><td>휴대폰</td><td>휴대폰 SMS 발송을 통한 접근 허용 방식</td></tr>
<tr><td>사무실 전화</td><td>사무실 전화 연결을 통한 접근 허용 방식(유료 구독 필수)</td></tr>
<tr><td>본인 확인 질문</td><td>사전에 등록한 사용자 질문 답변을 통한 접근 허용 방식</td></tr>
</table>
※ 암호 재설정 인증 필수 설정 기준
- 암호 재설정 인증 기준: 1단계 (전자 메일, 휴대폰)
- 암호 재설정 등록 기준: 사용자 로그인 시 등록 요구 (활성화), 인증 정보 확인 기간(90일)
- 암호 재설정 알림 기준: 암호가 재설정되는 경우 사용자에게 알림 활성화

※ 셀프 서비스 암호 재설정 기능은 프리미엄 구독을 신청한 경우에 사용이 가능함.</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 셀프 암호 재설정 기능 설정 방법
1) Azure Active Directory 메뉴 내 암호 재설정 기능 선택
 
</td></tr>
</table>

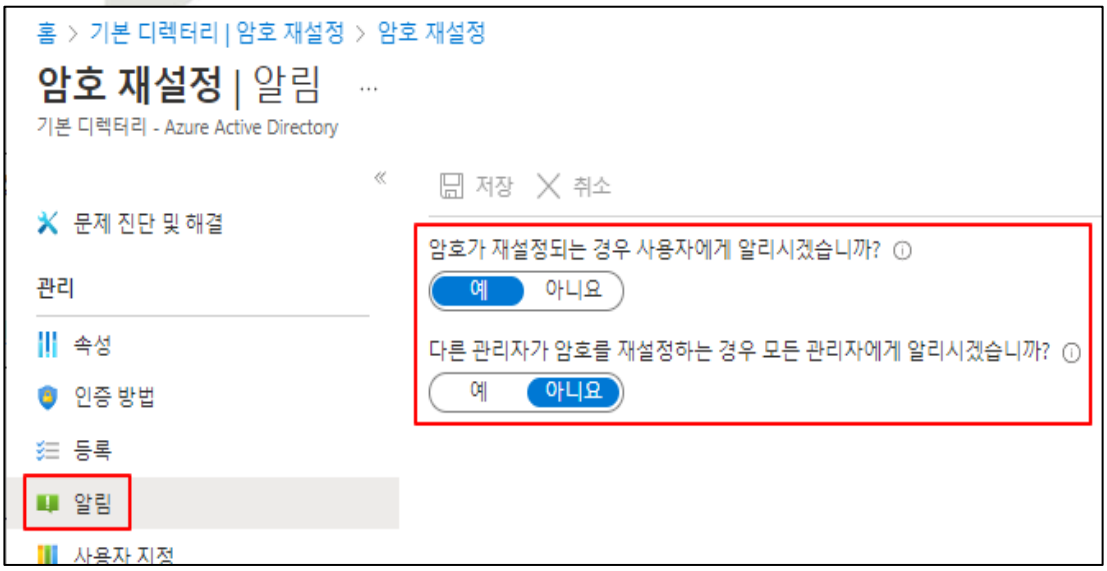
2) 속성 메뉴 내 셀프 서비스 암호 재설정 설정

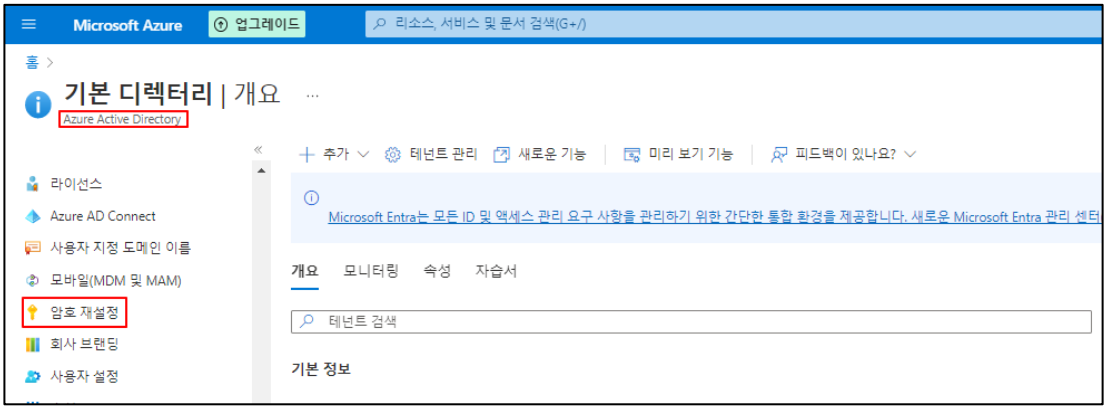
나. 정보 변경 시 사용자 알람 기능 설정 방법

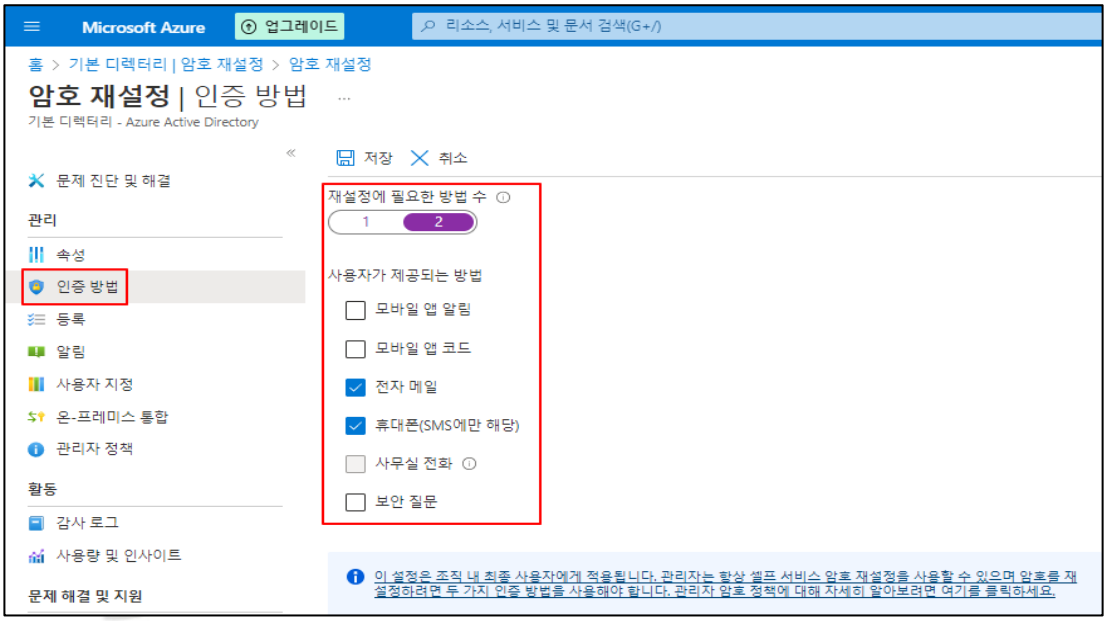
1) Azure Active Directory 메뉴 내 암호 재설정 기능 선택



2) 속성 메뉴 내 알림 설정



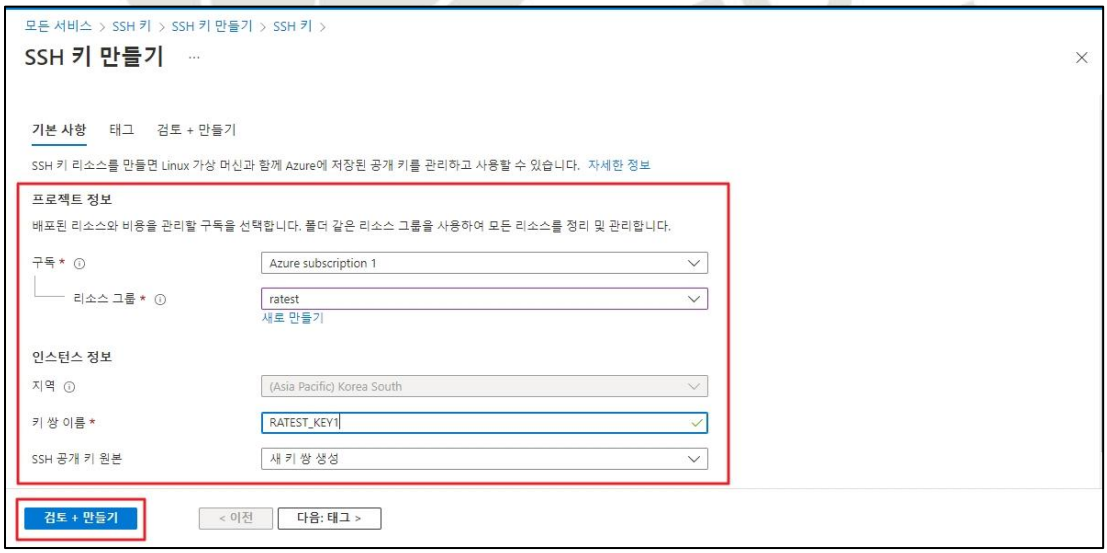
<table>
<tr>
<td></td>
<td>
다. 인증 방법 설정 방법
1) Azure Active Directory 메뉴 내 암호 재설정 기능 선택


2) 인증 방법 메뉴 내 인증 방법 설정


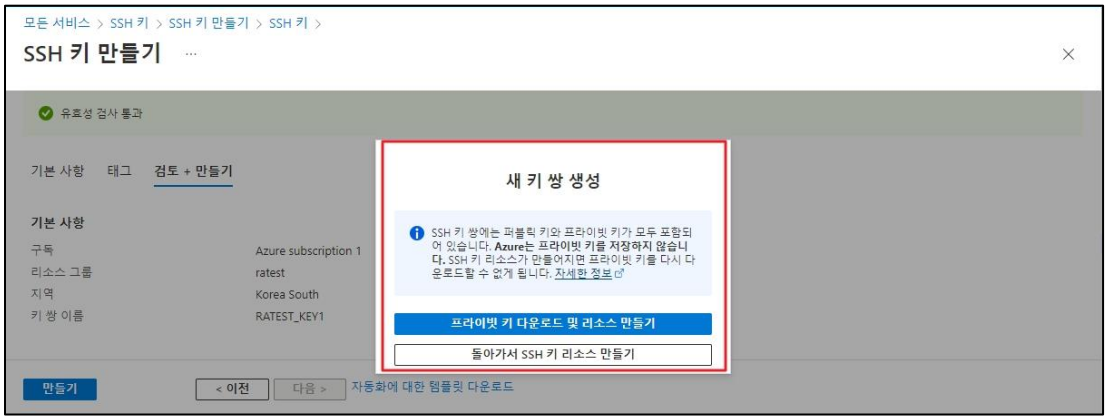
</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 암호 재설정 규칙이 필수 설정 기준에 맞게 설정되어 있는 경우

취약기준
: 암호 재설정 규칙이 필수 설정 기준에 맞게 설정되어 있지 않은 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

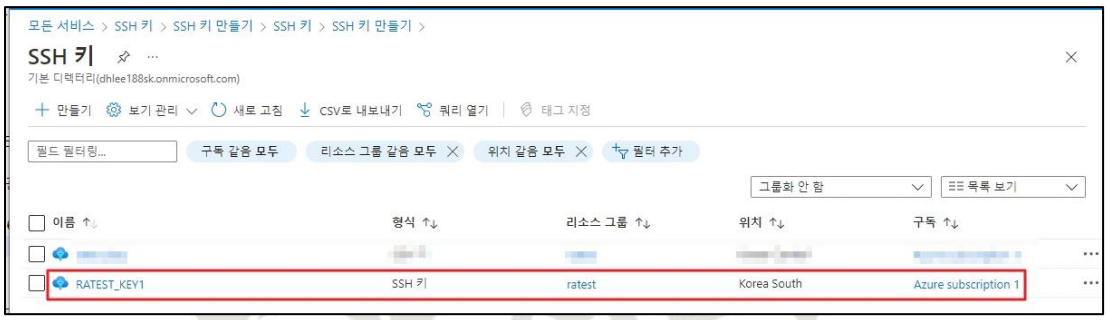
1.6 SSH Key 접근 관리

분류	계정 관리	중요도	하
항목명	SSH Key 접근 관리		
항목 설명	SSH 키는 기존의 "키 페어(pem)"와 동일한 방식의 공개-개인 키 쌍을 사용하여 SSH를 통해 가상머신으로 직접 접근이 가능합니다. SSH 키는 AZURE 포탈을 통해 생성 할 수 있으며 해당 키는 가상 머신에 적용하여 사용할 수 있습니다. 이에 불필요한 사용자 및 비인가된 사용자가 액세스 제어(IAM) 사용자/그룹 역할이 적용될 경우 가상머신 리소스에 접근이 가능해지는 문제가 발생할 수 있습니다.		
설정 방법	**가. SSH 키 추가 및 액세스 제어(IAM) 역할 할당** 1) SSH 키 추가  2) SSH 키 정보 입력 및 만들기  		

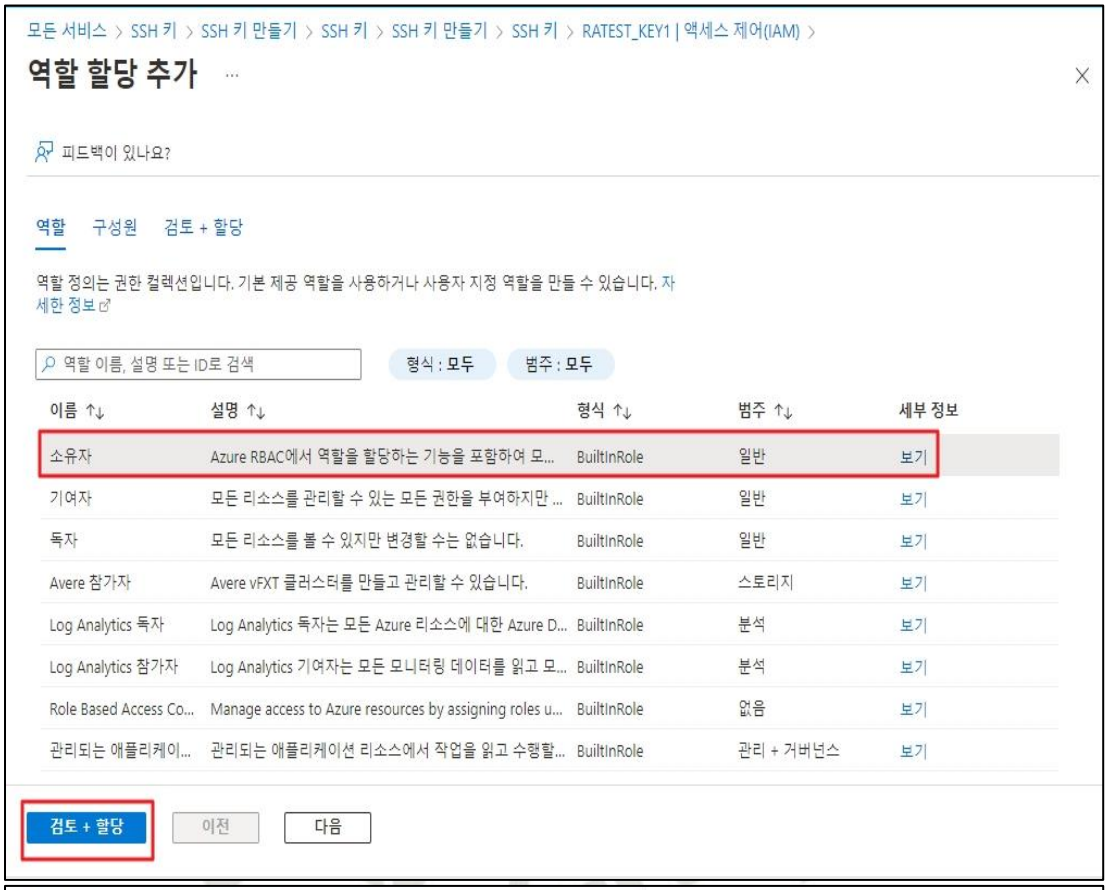
3) 프라이빗 키 별도 다운로드

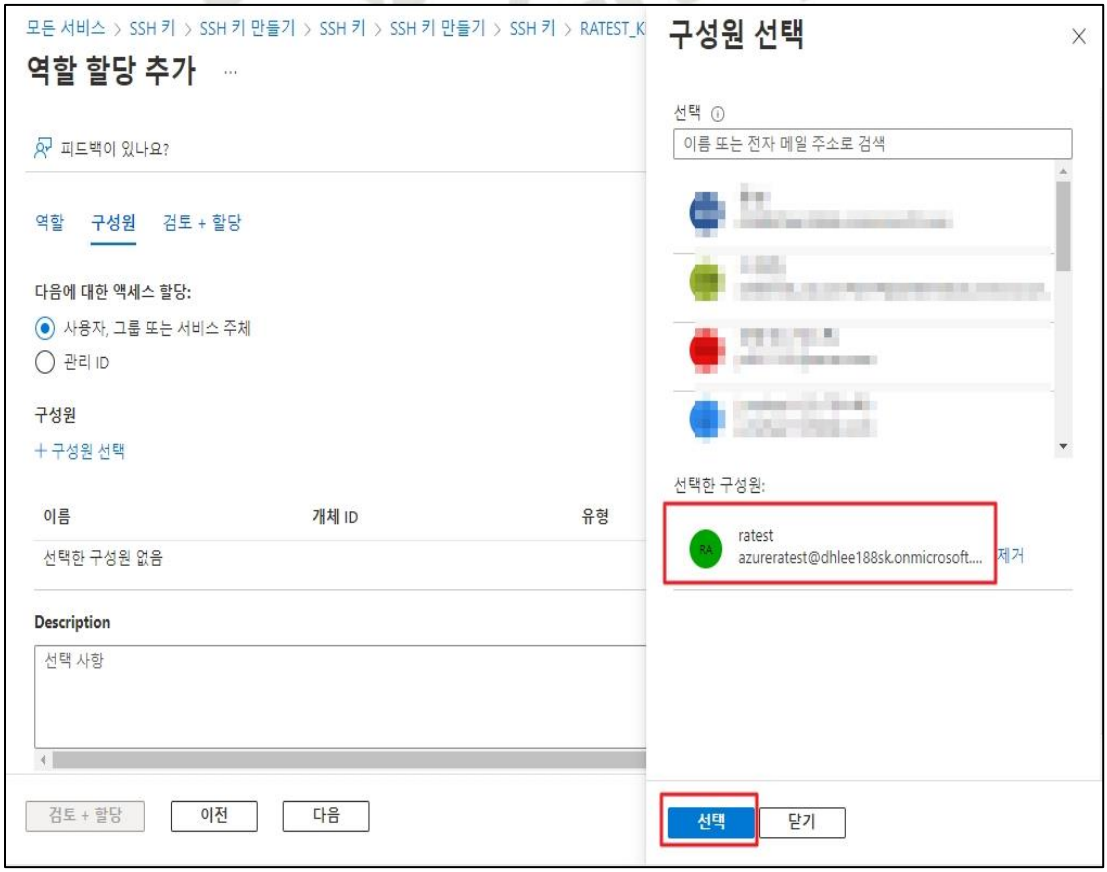


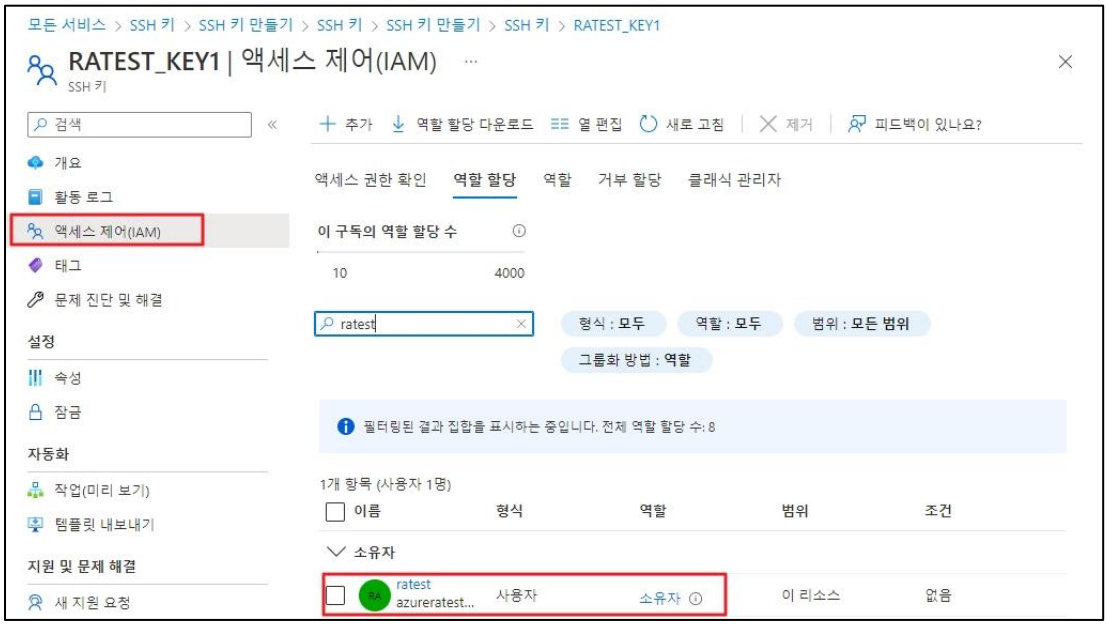
4) 생성된 SSH 키 확인



5) SSH 키의 액세스 제어(IAM) 역할 할당 추가

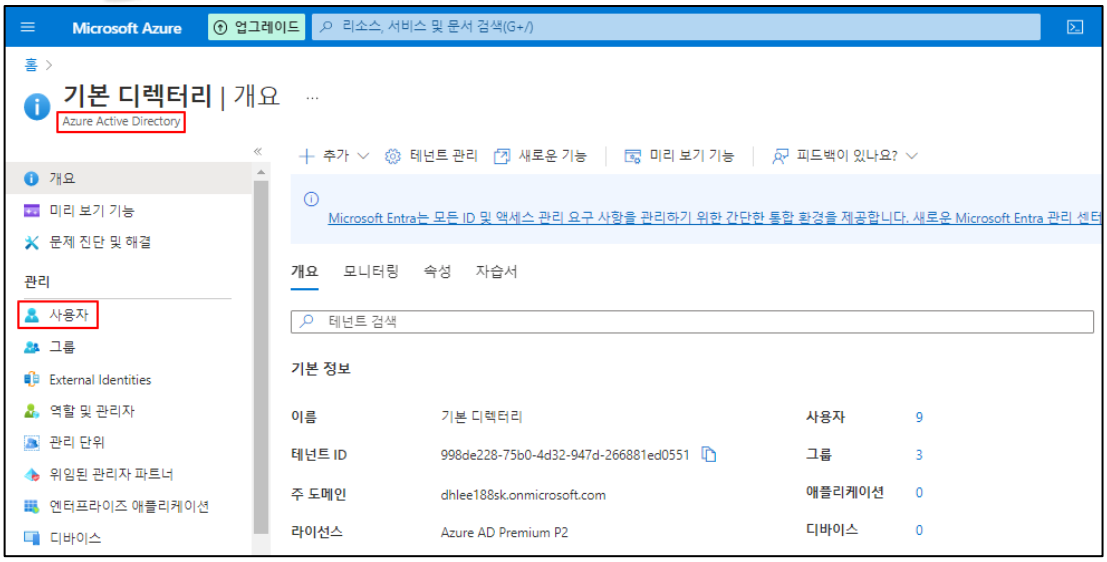

모든 서비스 > SSH 키 > SSH 키 만들기 > SSH 키 > SSH 키 만들기 > SSH 키 > RATEST_KEY1 | 액세스 제어(IAM) >
역할 할당 추가
피드백이 있나요?
역할
구성원
검토 + 할당
역할 정의는 권한 컬렉션입니다. 기본 제공 역할을 사용하거나 사용자 지정 역할을 만들 수 있습니다. 자세한 정보
역할 이름, 설명 또는 ID로 검색
형식 : 모두
범주 : 모두
이름
설명
형식
범주
세부 정보
소유자
Azure RBAC에서 역할을 할당하는 기능을 포함하여 모...
BuiltInRole
일반
보기
기여자
모든 리소스를 관리할 수 있는 모든 권한을 부여하지만 ...
BuiltInRole
일반
보기
독자
모든 리소스를 볼 수 있지만 변경할 수는 없습니다.
BuiltInRole
일반
보기
Avere 참가자
Avere vFXT 클러스터를 만들고 관리할 수 있습니다.
BuiltInRole
스토리지
보기
Log Analytics 독자
Log Analytics 독자는 모든 Azure 리소스에 대한 Azure D...
BuiltInRole
분석
보기
Log Analytics 참가자
Log Analytics 기여자는 모든 모니터링 데이터를 읽고 모...
BuiltInRole
분석
보기
Role Based Access Co...
Manage access to Azure resources by assigning roles u...
BuiltInRole
없음
보기
관리되는 애플리케이...
관리되는 애플리케이션 리소스에서 작업을 읽고 수행할...
BuiltInRole
관리 + 거버넌스
보기
검토 + 할당
이전
다음


모든 서비스 > SSH 키 > SSH 키 만들기 > SSH 키 > SSH 키 만들기 > SSH 키 > RATEST_K
역할 할당 추가
피드백이 있나요?
역할
구성원
검토 + 할당
다음에 대한 액세스 할당:
사용자, 그룹 또는 서비스 주체
관리 ID
구성원
+ 구성원 선택
이름
개체 ID
유형
선택한 구성원 없음
Description
선택 사항
검토 + 할당
이전
다음
구성원 선택
선택
이름 또는 전자 메일 주소로 검색
선택한 구성원:
ratest
azureratest@dhlee188sk.onmicrosoft....
제거
선택
닫기

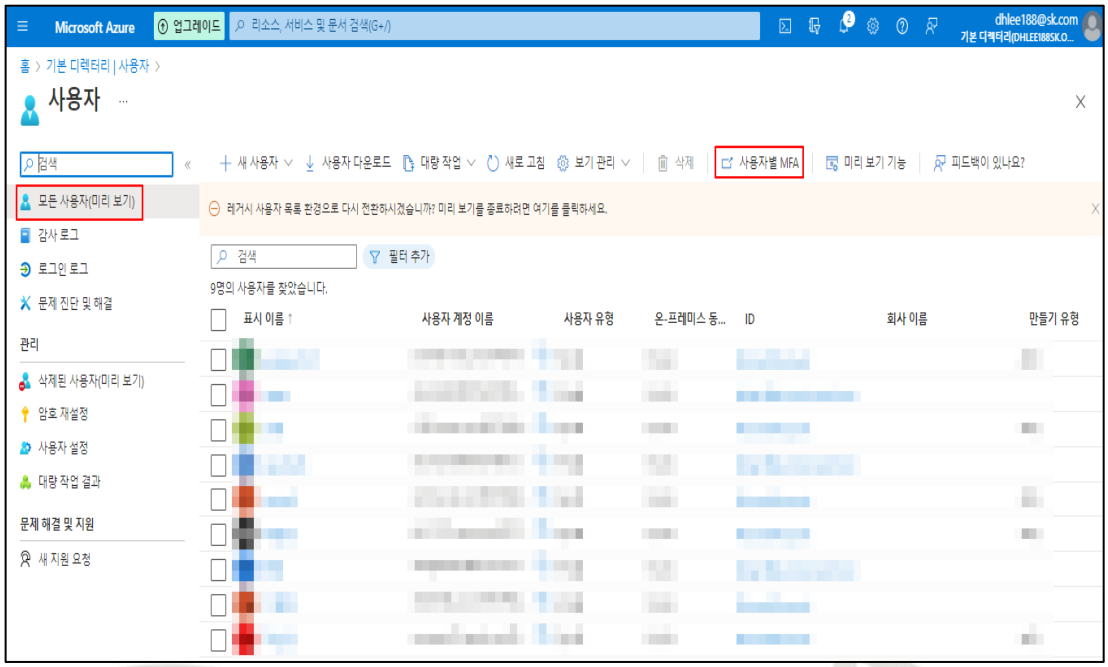
	6) SSH 키의 액세스 제어(IAM) 리스트 확인 
진단 기준	**양호기준** : SSH Key '생성/변경/삭제'가 관리자 및 소유자 계정만 가능하도록 설정되어 있을 경우 **취약기준** : SSH Key '생성/변경/삭제'가 관리자 및 소유자 계정만 가능하도록 설정되어 있지 않을 경우
비고	

1.7 MFA (Multi-Factor Authentication) 설정

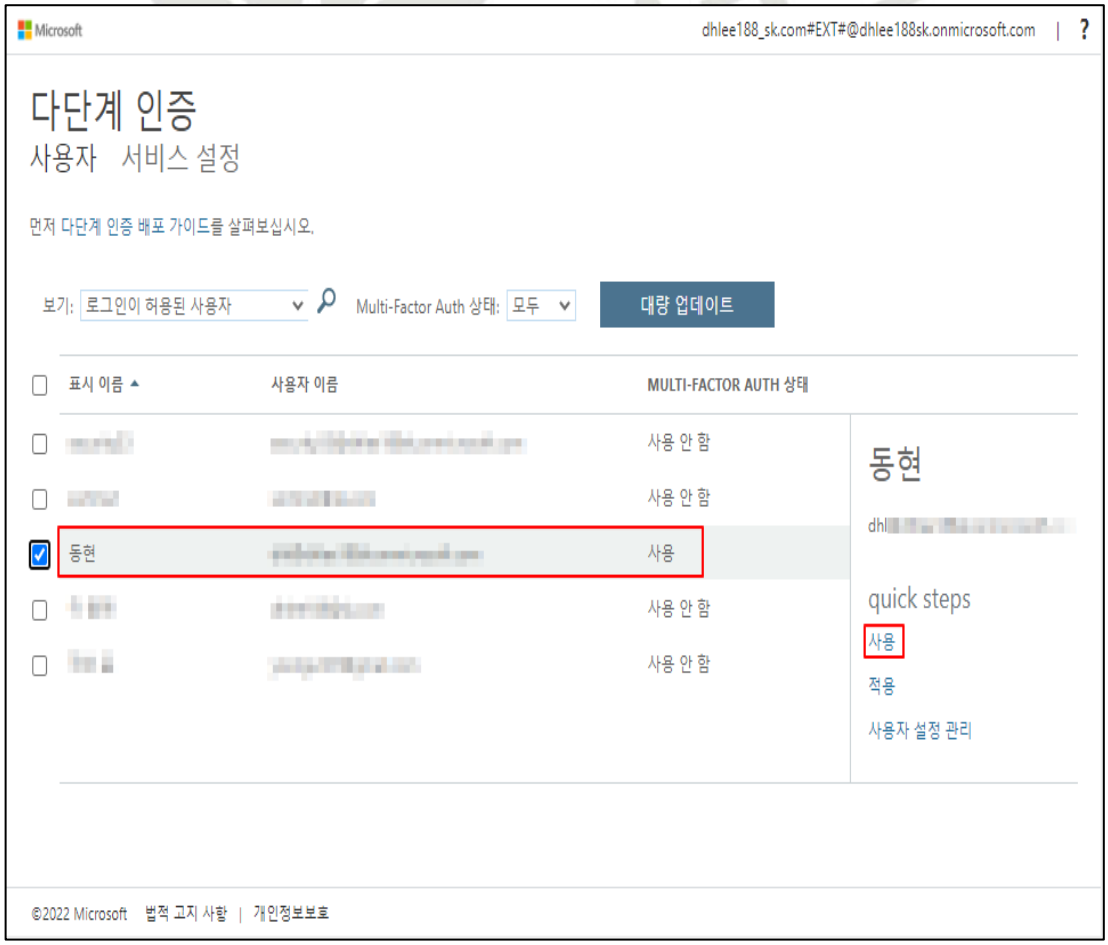
<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">MFA (Multi-Factor Authentication) 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">MFA(2차 인증방식)의 보안은 계층화된 접근 방식을 기반으로 합니다. MFA는 일반 사용자에게도 사용을 통해 관리계정 보안을 향상시킬 수 있으며 특히 관리자 계정에 MFA를 설정할 경우 Azure 리소스 생성/관리보안도 함께 강화할 수 있습니다.

※ MFA 구성 설정
<table>
<tr><th>기능</th><th>설명</th></tr>
<tr><td>계정잠금</td><td>거부된 인증 시도가 너무 많은 경우 MFA 서비스에서 계정을 일시적으로 잠급니다. 이 기능은 인증을 위해 PIN을 입력하는 사용자에게만 적용됩니다.
※ 계정잠금 기능은 프리미엄 구독을 신청한 경우에 사용이 가능함.</td></tr>
<tr><td>사용자 차단
/ 차단 해제</td><td>특정 사용자가 Multi-factor Authentication 요청을 받을 수 없도록 차단 하는 데 사용 합니다. 차단된 사용자에 대한 모든 인증 시도가 자동으로 거부됩니다. 사용자는 차단된 시간 이후 90일 동안 차단된 상태로 유지됩니다.</td></tr>
<tr><td>사기 행위 경고</td><td>사용자가 사기성 확인 요청을 보고서 수와 관련 된 설정 구성</td></tr>
<tr><td>알림</td><td>MFA 서버의 이벤트 알림이 가능하도록 설정합니다.</td></tr>
<tr><td>OAUTH 토큰</td><td>클라우드 기반 Azure MFA 환경에 사용되어 사용자의 OAUTH 토큰을 관리합니다.</td></tr>
<tr><td>전화 통화 설정</td><td>클라우드 및 온-프레미스 환경의 인사말 및 전화 통화 관련 설정을 구성합니다.</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. MFA 설정 방법 (Azure Active Directory 계정)
1) Azure Active Directory 메뉴 내 사용자 기능 선택
 
</td></tr>
</table>

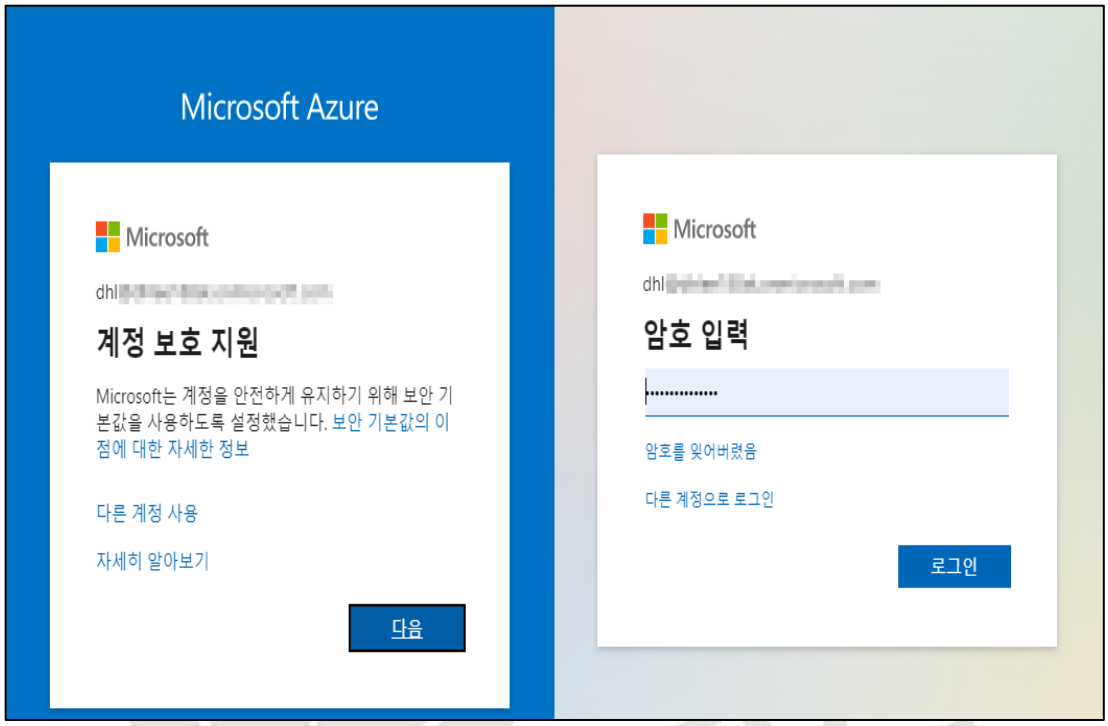
2) 모든 사용자 메뉴 내 사용자 별 MFA 선택



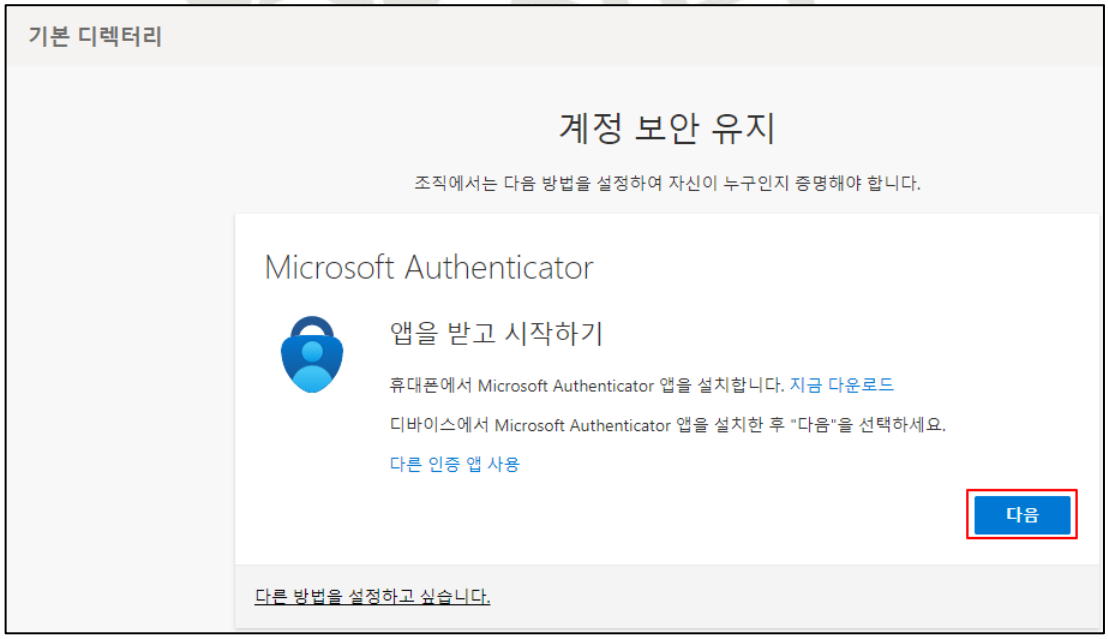
3) 다단계 인증 내 MFA를 사용할 사용자 선택 및 사용 버튼 클릭

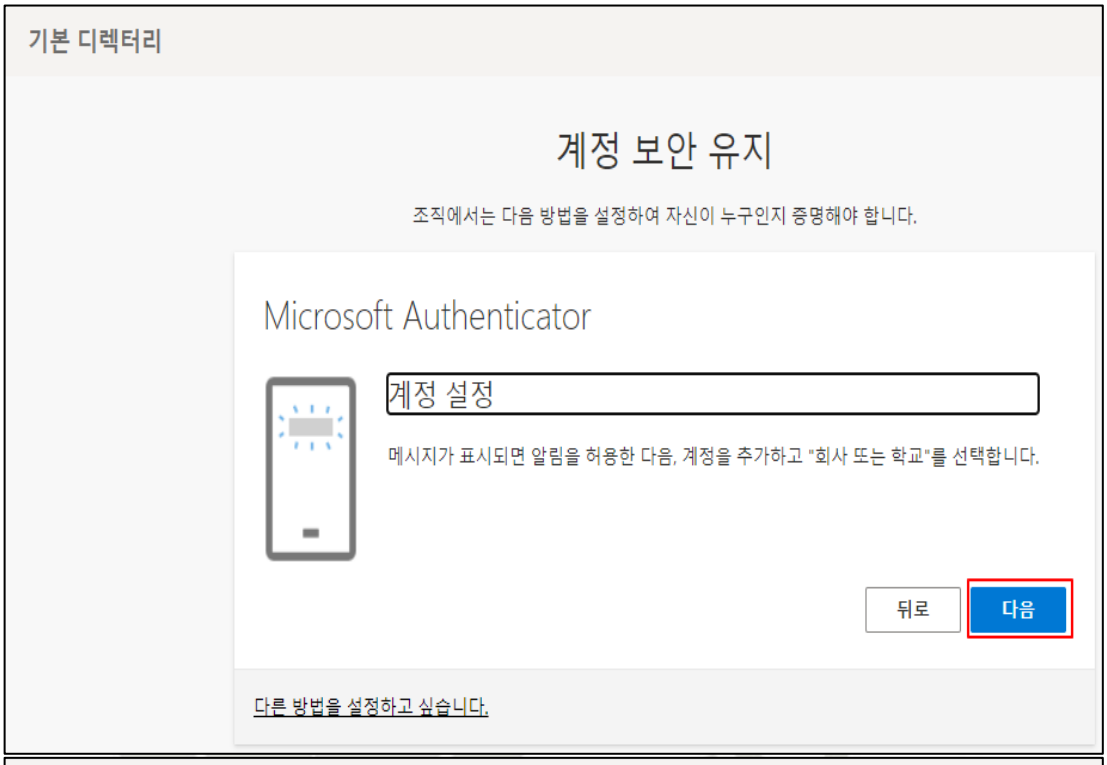


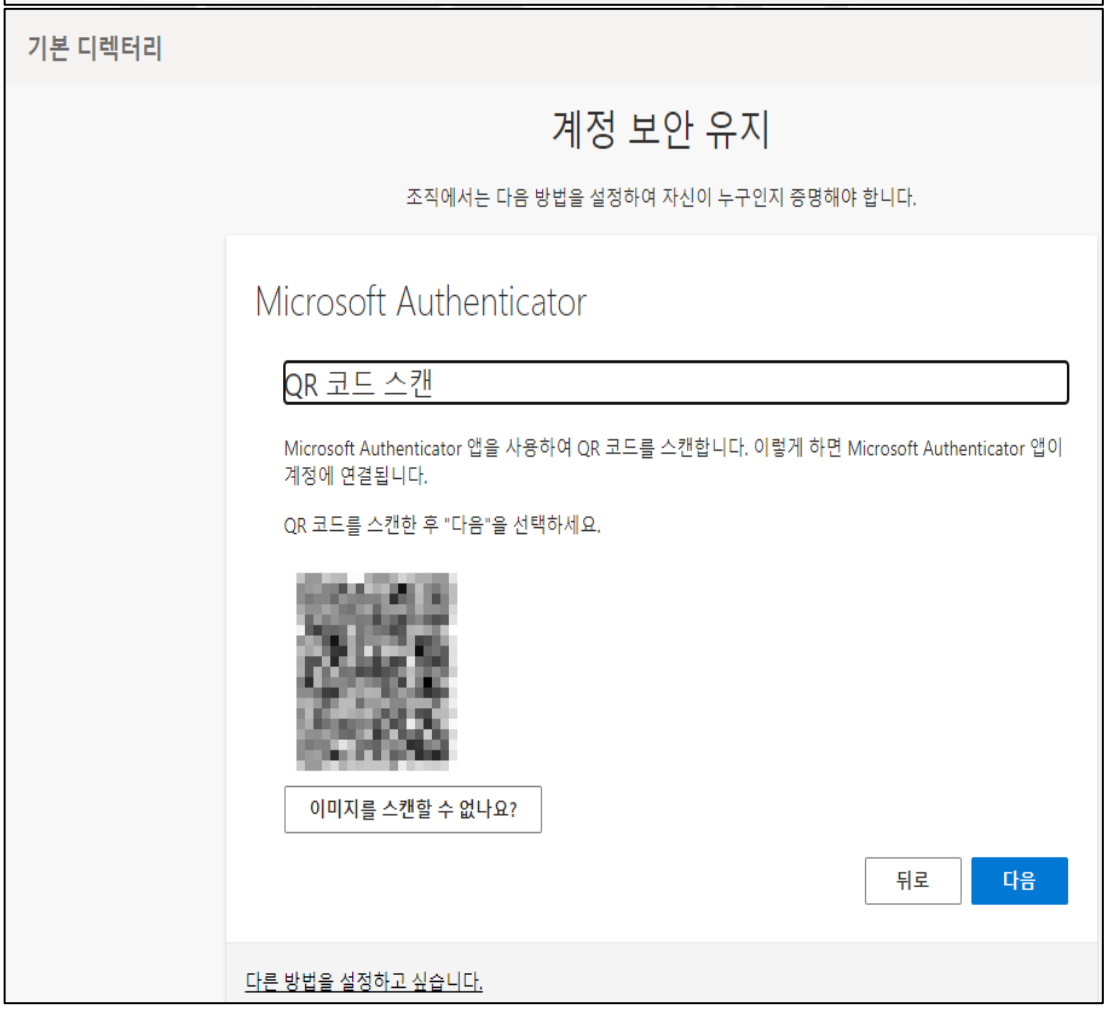
4) AD 계정으로 Azure 로그인 시도



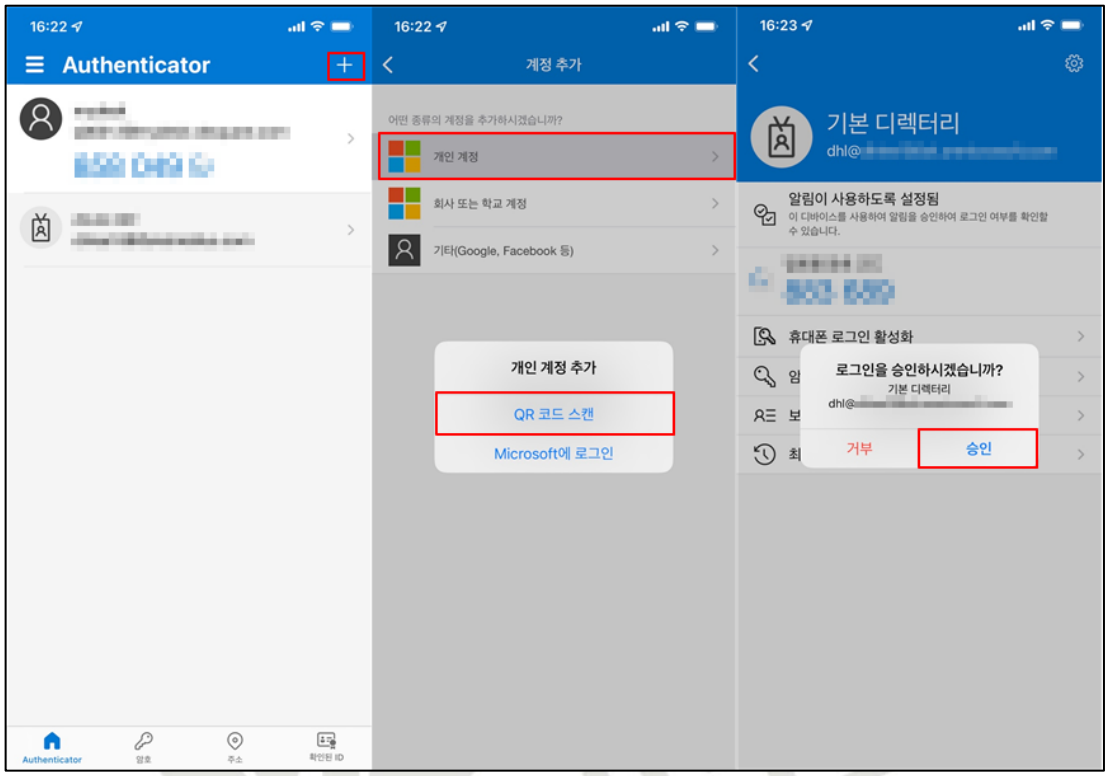
5) MFA에 사용될 Microsoft Authenticator 앱 시작하기



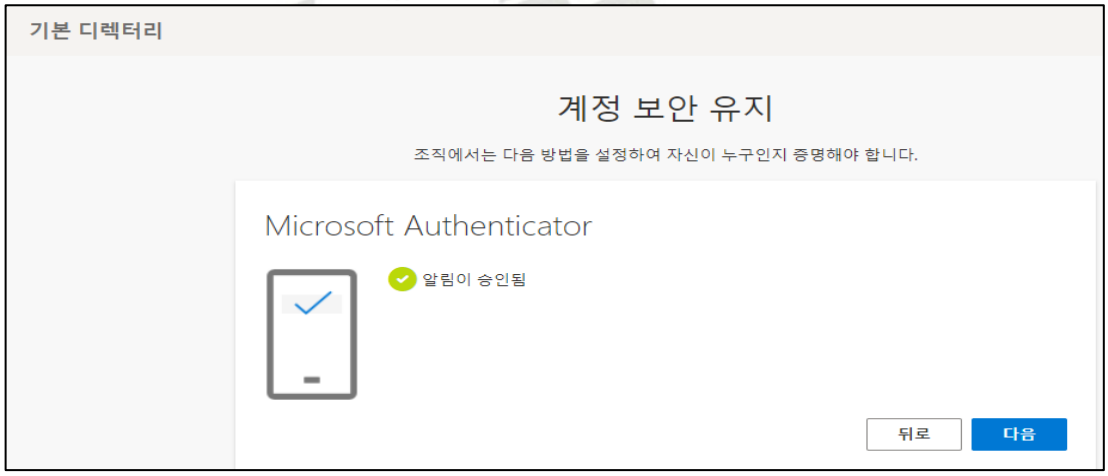


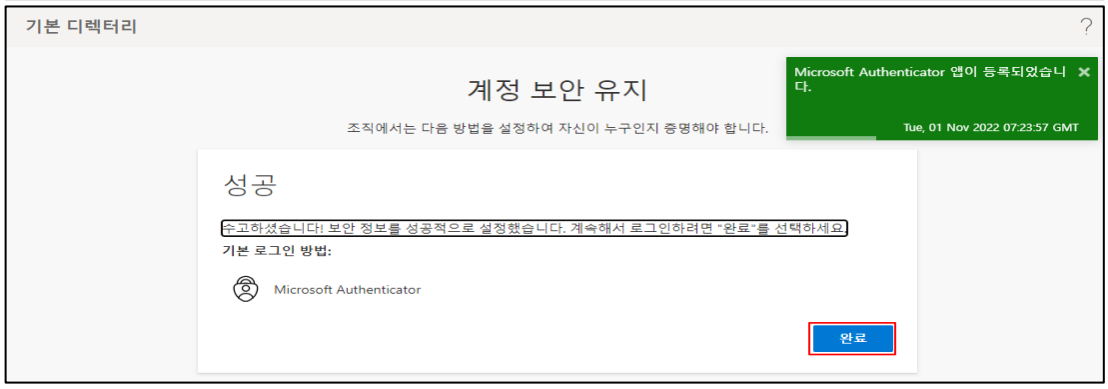


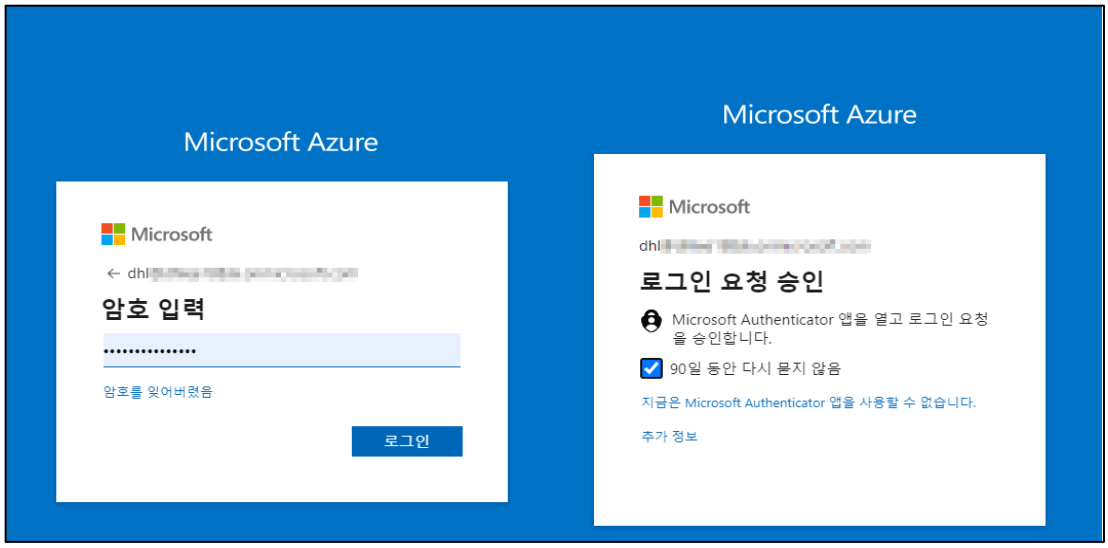
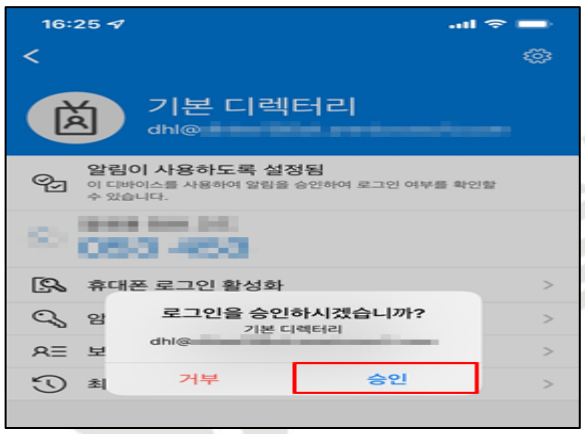
6) 모바일 앱 설치 후 QR 코드 스캔



7) 모바일 앱 인증 알림 승인 완료





	8) AD 계정으로 Azure 로그인 재 진행  9) 휴대폰으로 발송된 요청 승인 시 MFA를 통한 로그인 가능 
진단 기준	**양호기준** : AD 사용자 계정에 MFA를 활성화하여 사용하고 있을 경우 **취약기준** : AD 사용자 계정에 MFA를 활성화하여 사용하고 있지 않을 경우
비고	

1.8 MFA 계정 잠금 정책 관리

<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">MFA 계정 잠금 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Active Directory 사용자 계정 로그인 시 Multi-Factor-Authentication 인증에 대해 연속적으로 거부된 인증 시도가 많을 경우 계정을 일시적으로 잠글 수 있도록 정책을 적용할 수 있습니다. 해당 정책을 통해 1차 계정 인증을 통과하더라도 2차 인증을 연속으로 접근하게 될 경우를 차단하는 정책으로 계정 로그인의 보안을 강화할 수 있습니다. 해당 서비스는 Multi-Factor-Authentication 인증을 통해 PIN을 입력하는 사용자에게만 적용됩니다.

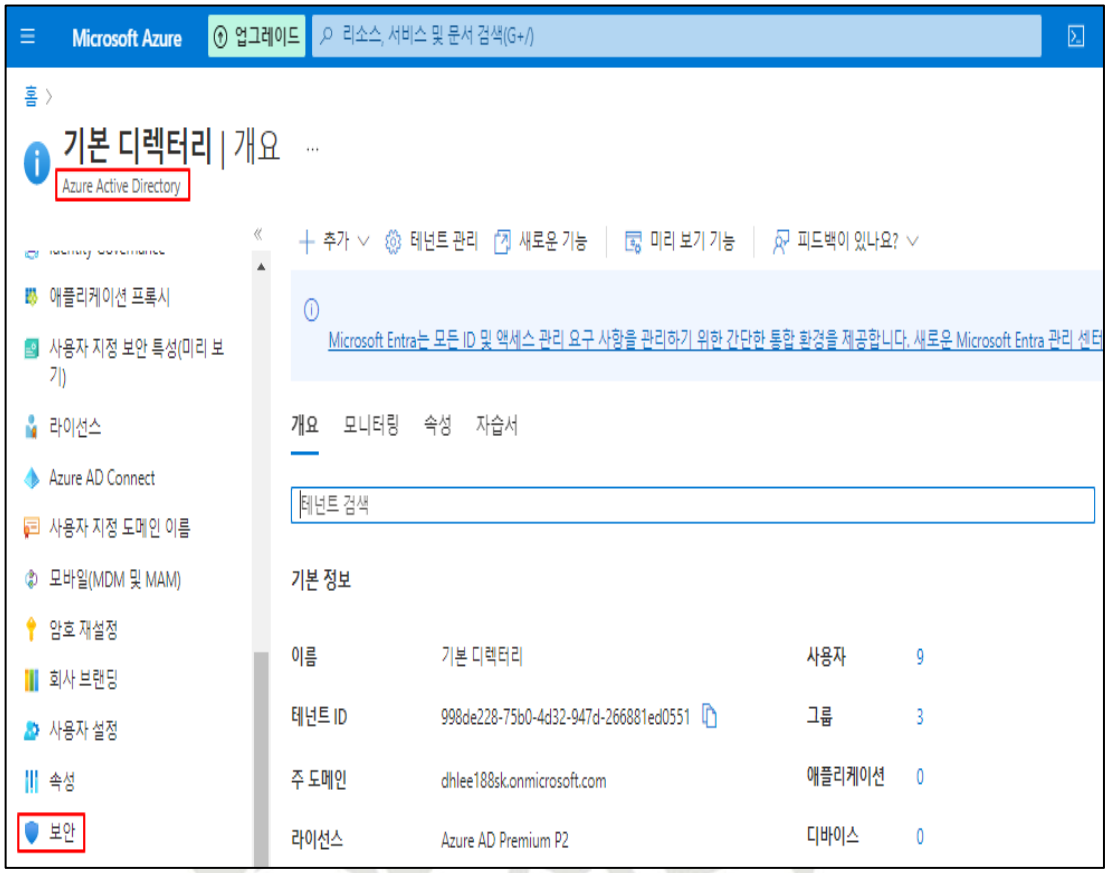
Azure에 접근하는 MS계정 및 Azure AD 계정의 암호 설정 시 유추하기 쉬운 암호를 설정하는 경우 비인가된 사용자가 해당 계정을 획득하여 접근할 가능성이 있으며, 계정을 생성할 경우 패스워드 정책을 정확히 반영하여 비인가된 사용자의 악의적인 계정탈취를 방지해야 합니다.

※ Multi-Factor-Authentication 계정 잠금 정책 기준
- 계정 잠금을 트리거하는 MFA 거부 수 (5회)
- 계정 잠금 카운터가 다시 설정될 때까지의 시간(분) (15분)
- 계정이 자동으로 차단 해제될 때까지의 시간(분) (60분)

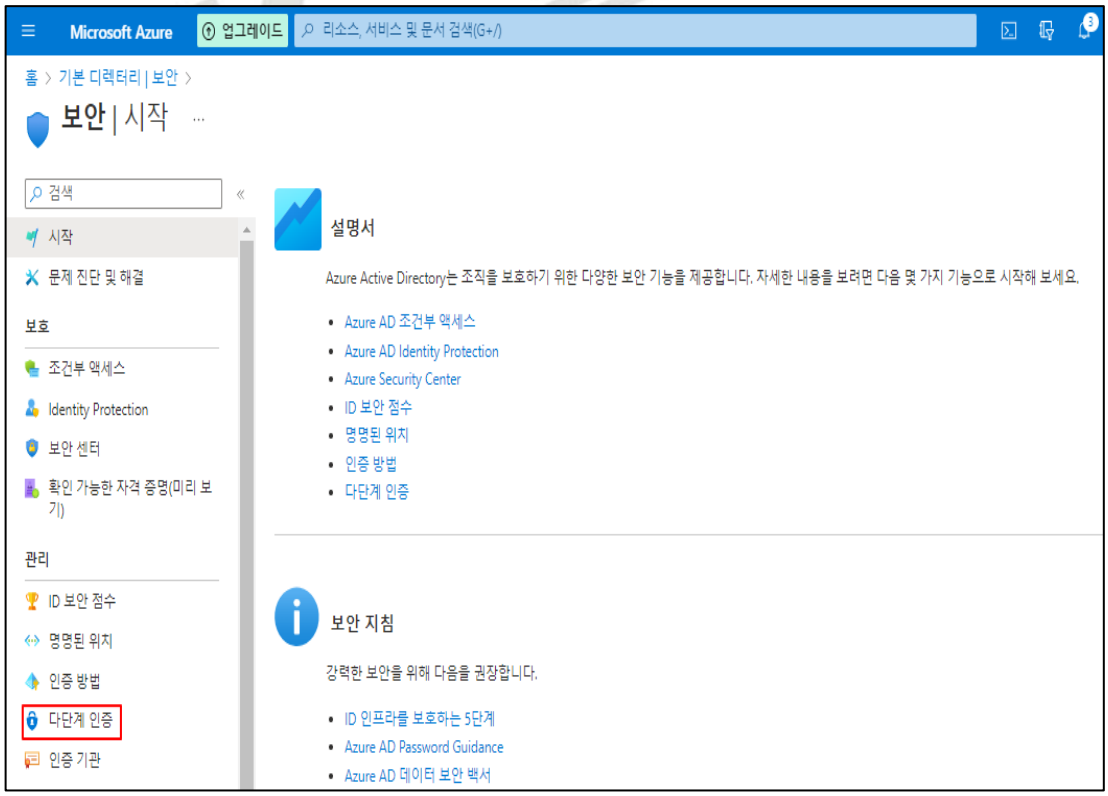
<패스워드 설정기준>
패스워드는 영문 대문자(26개), 영문 소문자(26개), 숫자(10개), 특수문자(32개)의 4종류
- 2종류 이상의 문자 구성과 8자리 이상의 길이로 구성된 문자열
- 10자리 이상의 길이로 구성된 문자열 (숫자로만 구성할 경우 취약할 수 있음)

<추측이 어렵도록 패스워드 반영 설계>
1) Null 패스워드 사용 금지
2) 문자 또는 숫자만으로 구성 금지
3) 사용자 ID와 동일한 패스워드 금지
4) 연속적인 문자 및 숫자 사용 금지
5) 주기성 패스워드 사용 금지
6) 전화번호, 생일, 계정명, Hostname과 같이 추측하기 쉬운 패스워드 사용 금지
※ 패스워드 설정 기준은 KISA "패스워드 선택 및 이용 안내서"를 참고함 (2019년 6월 개정)
https://seed.kisa.or.kr/kisa/Board/53/detailView.do

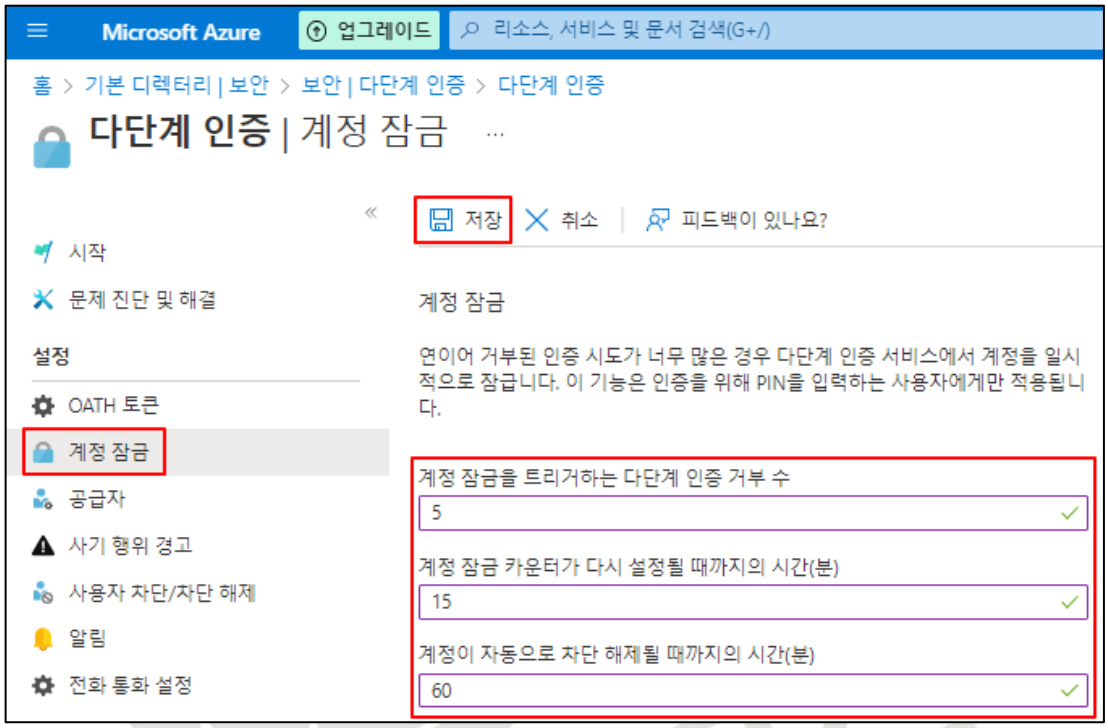
※ MS계정의 경우, 기본적으로 패스워드 복잡도 정책이 적용되어 있으며, 암호보안 설정을 통해 만기일 설정(72일)이 가능합니다.</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. MFA 계정 잠금 기능 설정 방법
1) Azure Active Directory 메뉴 내 보안 기능 선택</td></tr>
</table>


Microsoft Azure
업그레이드
리소스, 서비스 및 문서 검색(G+/)
홈 >
기본 디렉터리 | 개요
Azure Active Directory
추가
테넌트 관리
새로운 기능
미리 보기 기능
피드백이 있나요?
애플리케이션 프록시
사용자 지정 보안 특성(미리 보기)
라이선스
Azure AD Connect
사용자 지정 도메인 이름
모바일(MDM 및 MAM)
암호 재설정
회사 브랜딩
사용자 설정
속성
보안
Microsoft Entra는 모든 ID 및 액세스 관리 요구 사항을 관리하기 위한 간단한 통합 환경을 제공합니다. 새로운 Microsoft Entra 관리 센터
개요
모니터링
속성
자습서
테넌트 검색
기본 정보
이름
기본 디렉터리
사용자
9
테넌트 ID
998de228-75b0-4d32-947d-266881ed0551
그룹
3
주 도메인
dhlee188sk.onmicrosoft.com
애플리케이션
0
라이선스
Azure AD Premium P2
디바이스
0

2) 다단계 인증 메뉴 선택

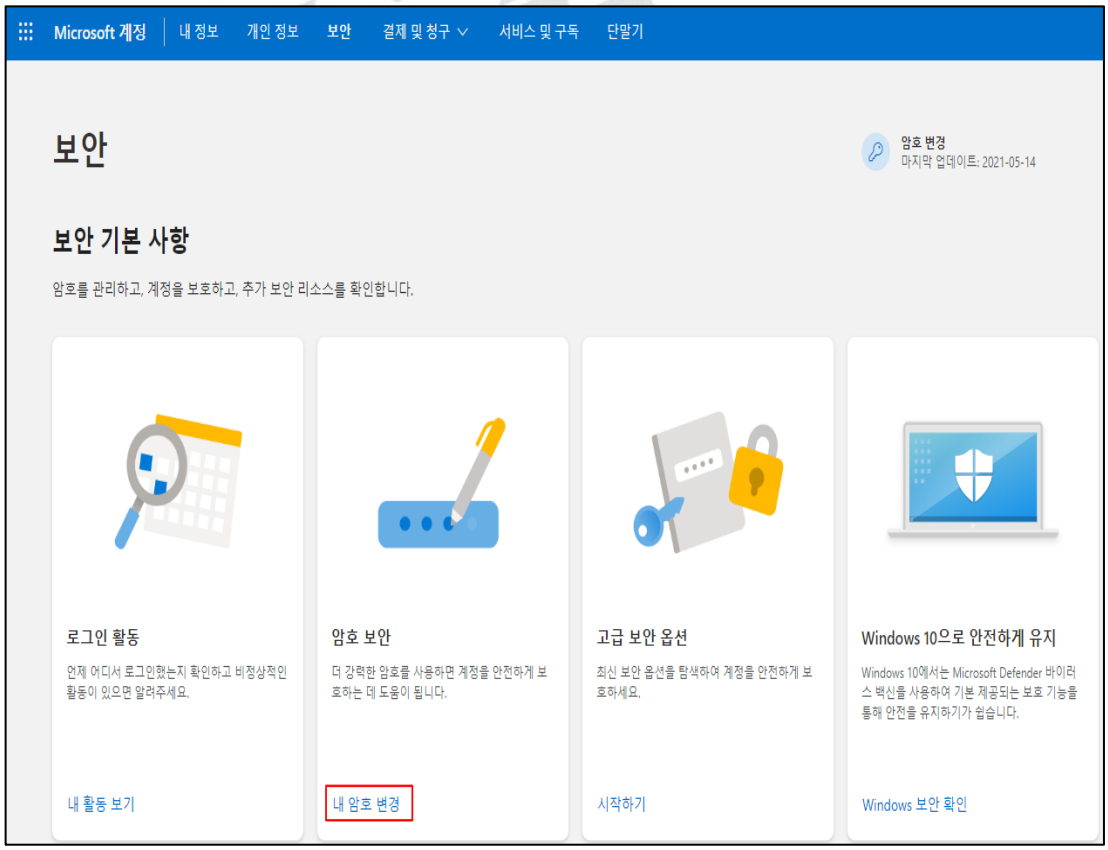

Microsoft Azure
업그레이드
리소스, 서비스 및 문서 검색(G+/)
홈 > 기본 디렉터리 | 보안 >
보안 | 시작
검색
시작
문제 진단 및 해결
보호
조건부 액세스
Identity Protection
보안 센터
확인 가능한 자격 증명(미리 보기)
관리
ID 보안 점수
명명된 위치
인증 방법
다단계 인증
인증 기관
설명서
Azure Active Directory는 조직을 보호하기 위한 다양한 보안 기능을 제공합니다. 자세한 내용을 보려면 다음 몇 가지 기능으로 시작해 보세요.
Azure AD 조건부 액세스
Azure AD Identity Protection
Azure Security Center
ID 보안 점수
명명된 위치
인증 방법
다단계 인증
보안 지침
강력한 보안을 위해 다음을 권장합니다.
ID 인프라를 보호하는 5단계
Azure AD Password Guidance
Azure AD 데이터 보안 백서

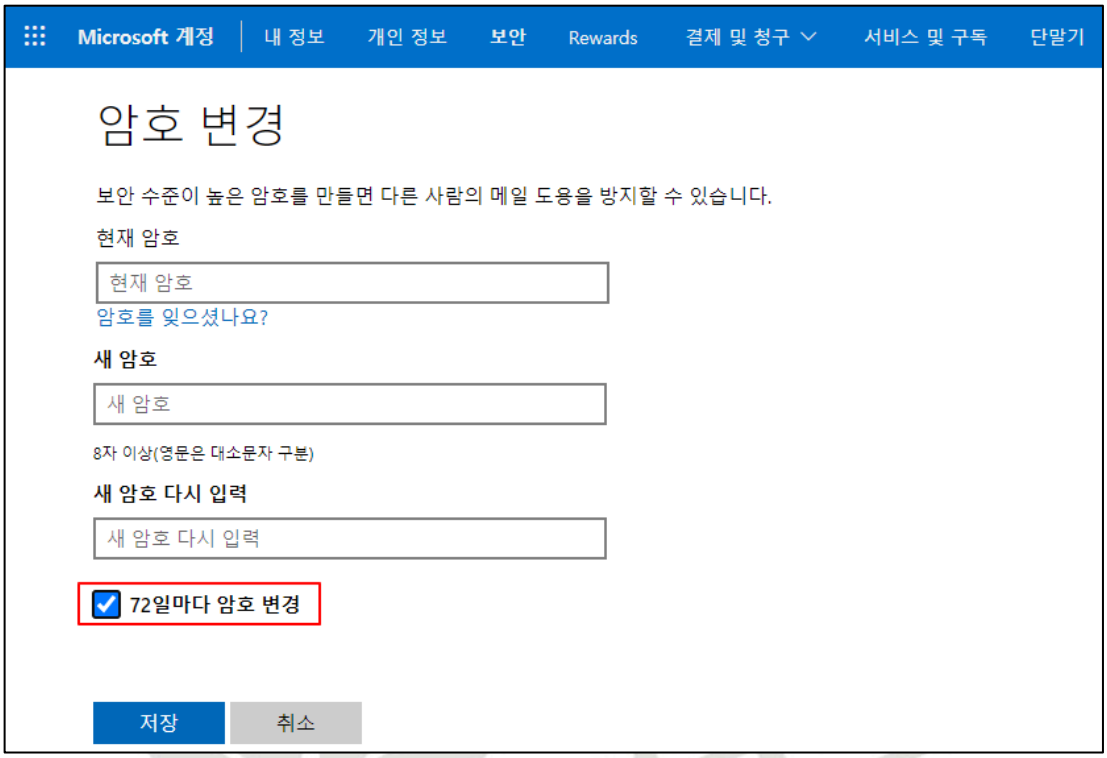
3) 계정 잠금 메뉴 내 값 설정 및 저장



나. MS 계정 암호 사용기간 만기 시 자동 변경 설정 방법

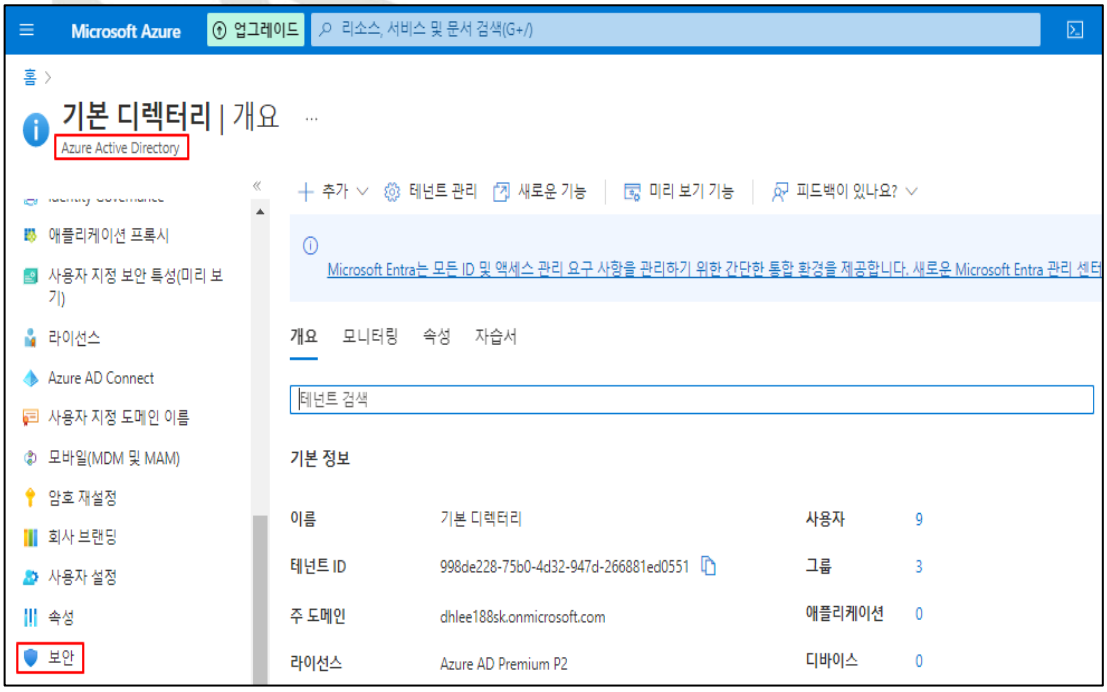
1) Microsoft 계정 메뉴 내 암호 보안 선택



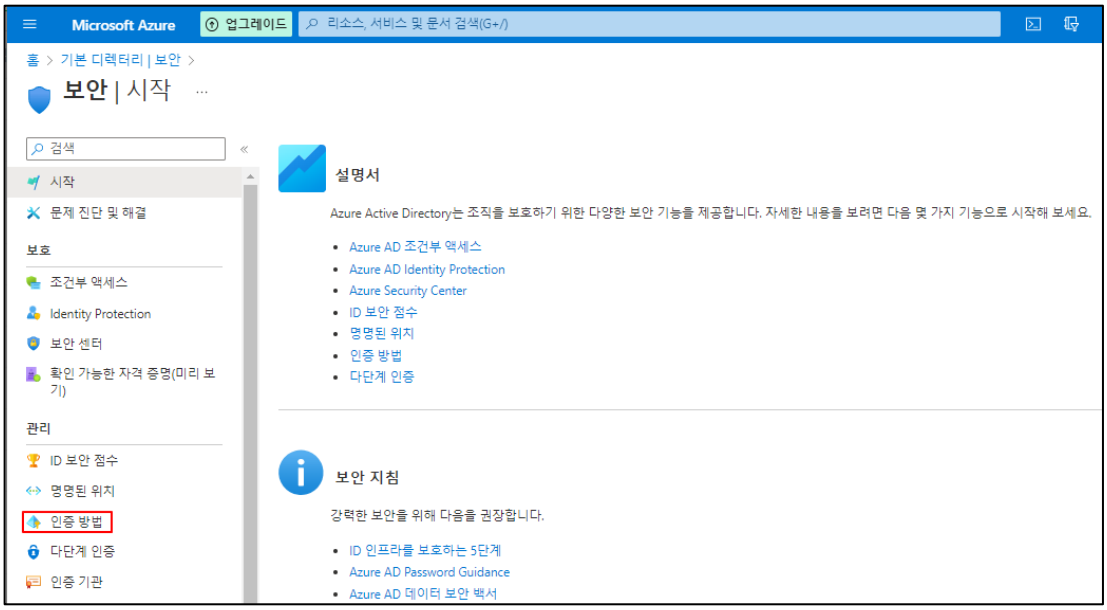
	2) 암호 변경 및 72일마다 암호변경 옵션 활성화 후 저장 
진단 기준	**양호기준** : 계정 잠금 설정이 정책에 맞게 설정되어 있을 경우 **취약기준** : 계정 잠금 설정이 정책에 맞게 설정되어 있지 않을 경우
비고	

1.9 Azure 패스워드 정책 관리

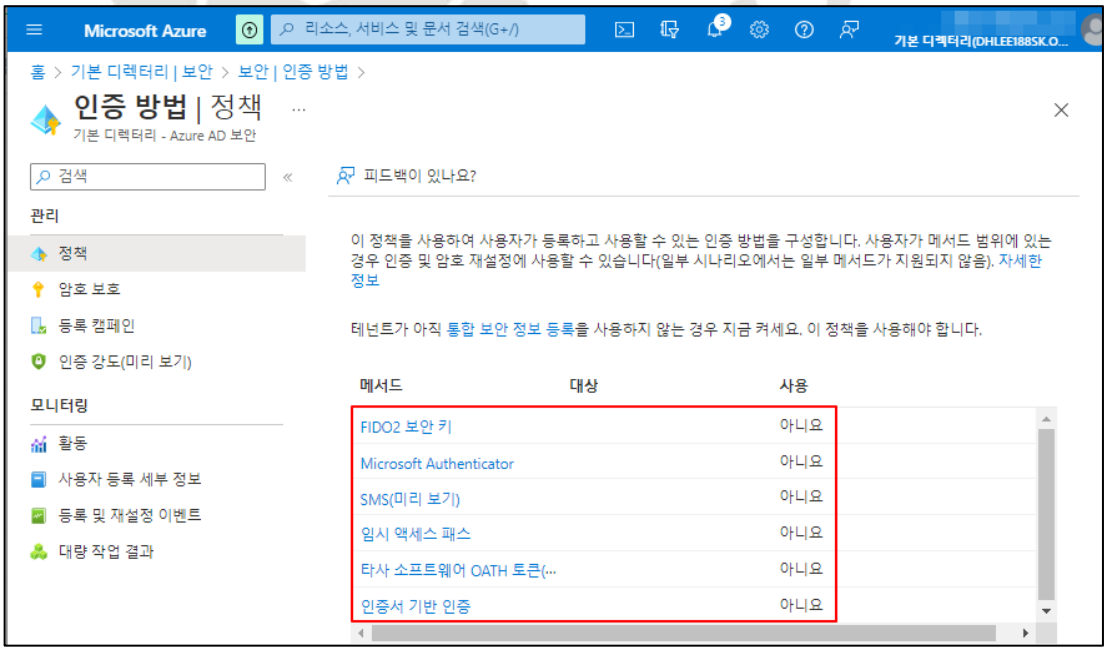
<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Azure 패스워드 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure AD(Activie Directory)에서 제공하는 인증방법을 통해 인증 정책을 설정하거나, 암호보호 정책을 설정할 수 있습니다. 인증방법 정책은 전체 또는 일부 사용자에게 암호가 아닌 다른 방식의 인증을 사용하도록 설정하는 기능이며, 암호보호 정책은 조직의 암호 정책을 강화할 수 있습니다.

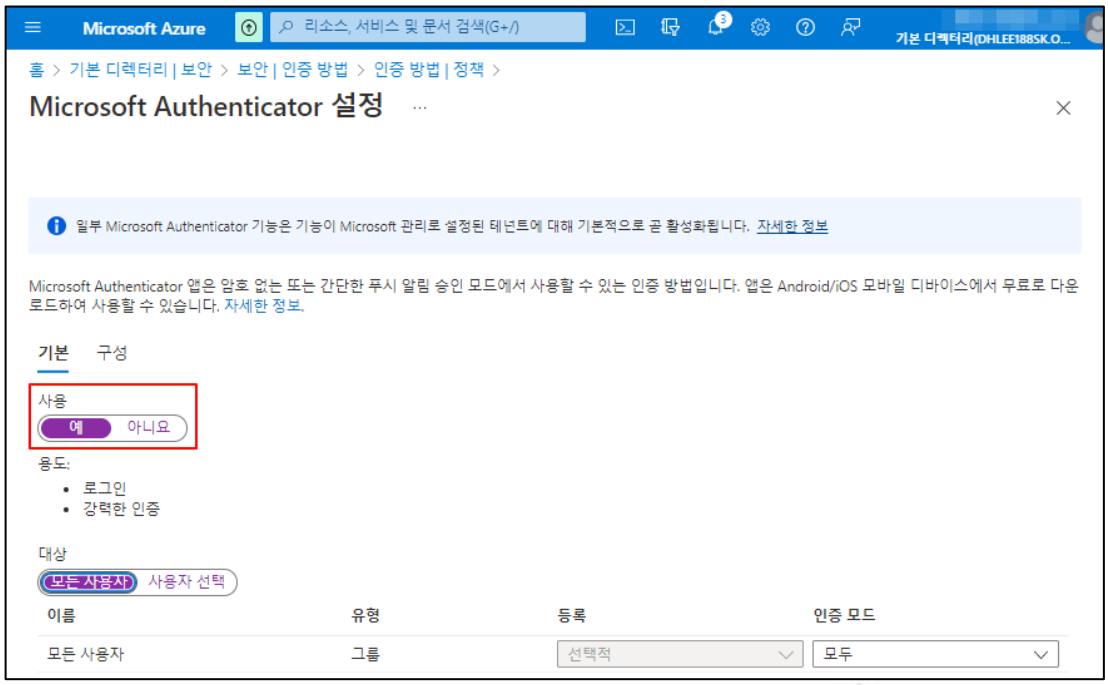
※ AD 인증방식 암호보호 정책
<table>
<tr><th>설정</th><th>내용</th><th>기준값</th></tr>
<tr><td>잠금 임계값</td><td>로그인 실패 시 허용 횟수</td><td>5회</td></tr>
<tr><td>잠금 시간(초)</td><td>계정 최초 잠금 시 잠금 시간이며, 실패횟수가 증가할수록 잠금 시간은 증가함.</td><td>3600초</td></tr>
<tr><td>사용자 지정 금지된 암호</td><td>추측하기 쉬운 암호의 사용을 금지하기 위해 암호 시스템에 관리자가 등록한 금지 암호를 등록</td><td>사용자 정의</td></tr>
<tr><td>Windows 서버 AD에 대한 암호보호</td><td>온-프레미스와 통합되어 있을 경우, Azure AD의 안전한 암호 배포를 위해 에이전트를 설치</td><td>예</td></tr>
<tr><td>모드</td><td>사용자 지정 금지된 암호를 사용할 경우 사용금지(적용됨) 또는 로그만 기록(감사)</td><td>적용됨</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 사용자 인증 설정 방법
1) Azure Active Directory 메뉴 내 보안 기능 선택
 
</td></tr>
</table>

2) 인증 방법 메뉴 선택



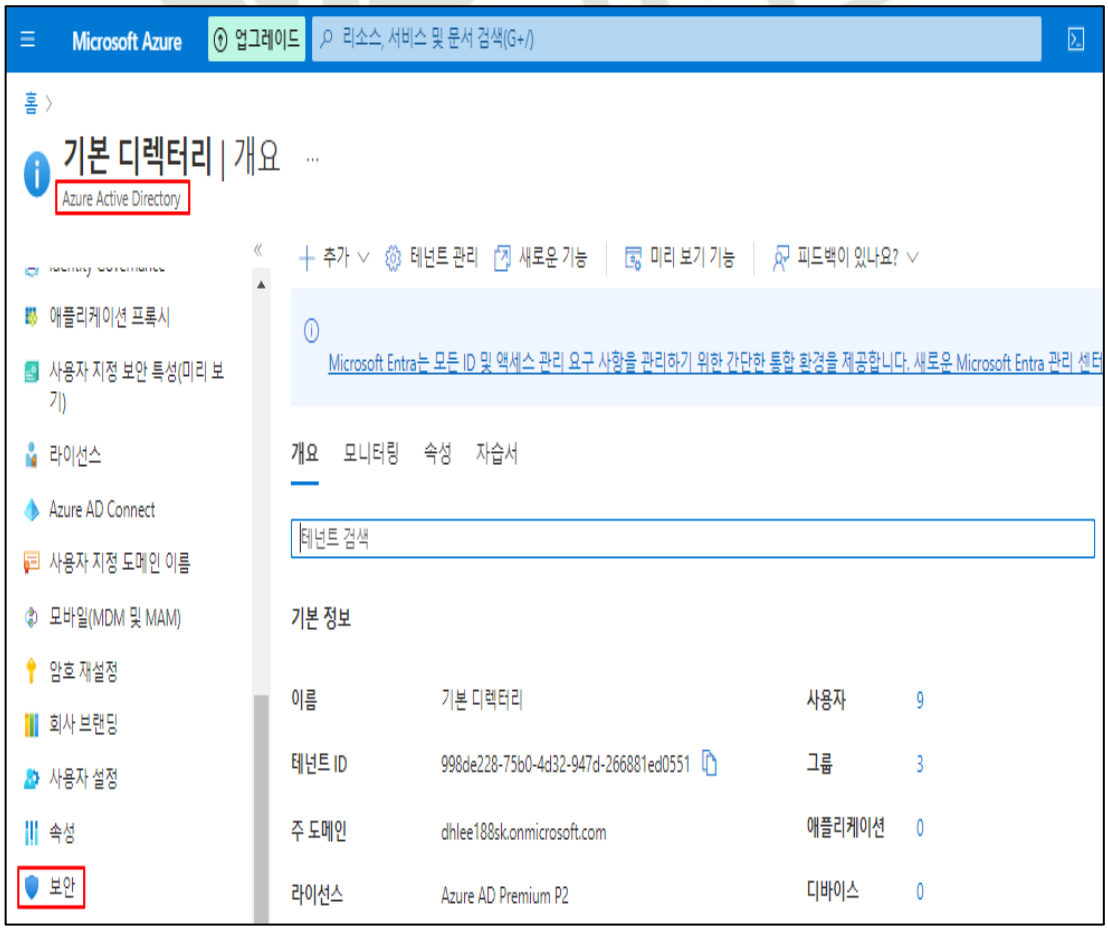
3) 인증 정책 중 Microsoft Authenticator 설정 활성화



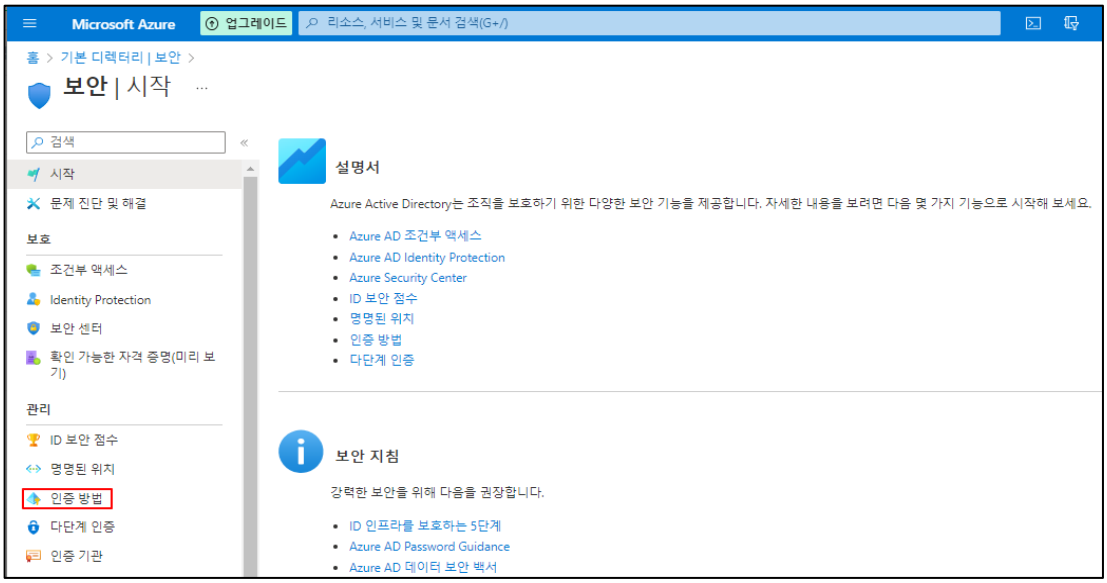


나. 로그인 정책 설정 방법

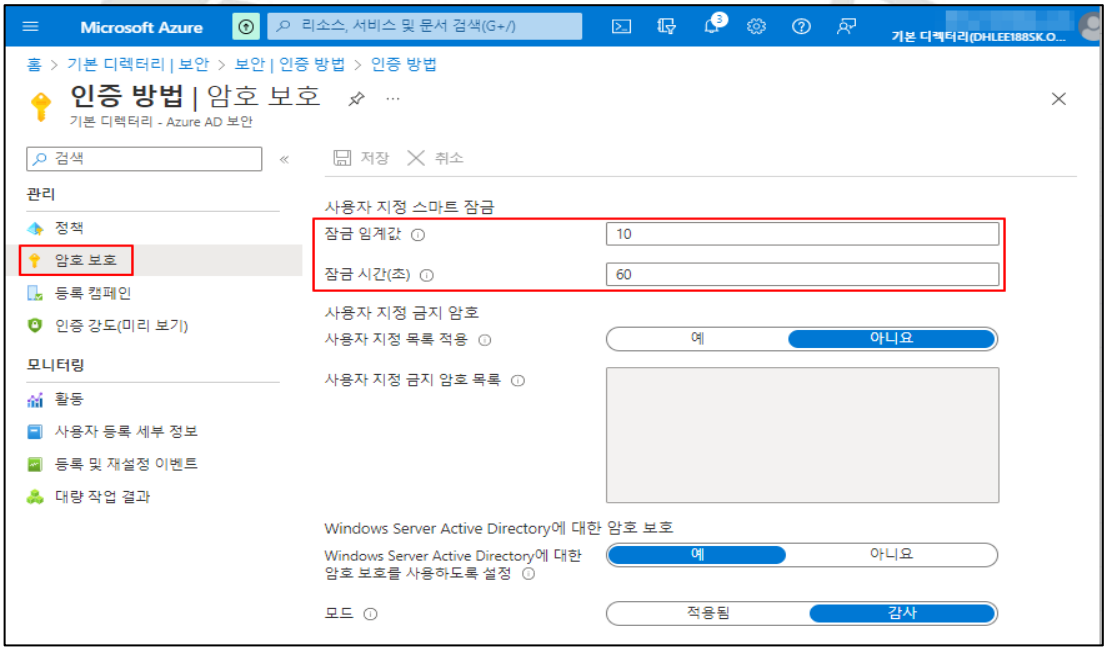
1) Azure Active Directory 메뉴 내 보안 기능 선택



2) 인증 방법 메뉴 선택



3) 암호 보호 메뉴 내 사용자 지정 스마트 잠금 설정



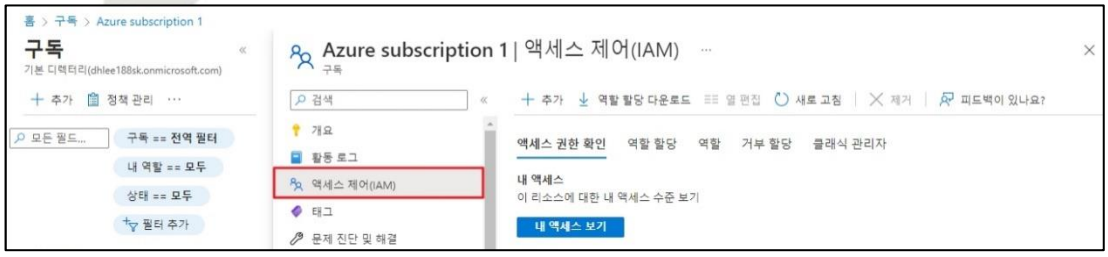
진단 기준	**양호기준** : 정책에 맞게 암호 보호 정책을 적용하여 사용하고 있을 경우 **취약기준** : 정책에 맞게 암호 보호 정책을 적용하여 사용하고 있지 않을 경우
비고	

2. 권한 관리

2.1 구독 액세스 제어(IAM) 역할 관리

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">구독 액세스 제어(IAM) 역할 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
모든 Azure 리소스는 논리적으로 하나의 구독과 연결됩니다. 리소스를 만들 때 해당 리소스를 배포할 Azure 구독을 선택합니다. 나중에 다른 구독으로 리소스를 이동할 수 있습니다.

"소유자/기여자/사용자 액세스 관리자" 권한은 IAM 계정 역할 중 가능 높은 권한들로 클라우드 리소스에 대한 전반적인 작업을 가능하게 합니다. 이처럼 높은 권한은 최소한의 관리자에게만 부여되어야 하며, 인가되지 않거나 불필요한 계정에 부여되지 않도록 해야 합니다.

※ IAM 사용자 역할(예시)
<table>
<tr><th>역할 이름</th><th>역할 구분</th><th>상세설명</th></tr>
<tr><td>소유자</td><td>일반</td><td>Azure RBAC 에서 역할을 할당하는 기능을 포함하여 모든 리소스를 관리할 수 있는 모든 권한을 부여합니다.</td></tr>
<tr><td>기여자</td><td>일반</td><td>모든 리소스를 관리할 수 있는 모든 권한을 부여하지만 Azure RBAC 에서 역할 할당, Azure Blueprints 에서 할당 관리 또는 이미지 갤러리 공유를 허용하지 않습니다.</td></tr>
<tr><td>사용자 액세스 관리자</td><td>일반</td><td>Azure 리소스에 대한 사용자 액세스를 관리할 수 있음</td></tr>
<tr><td>독자</td><td>일반</td><td>모든 리소스를 볼 수 있지만 변경할 수는 없습니다.</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">
가. 구독 액세스 제어(IAM) 역할 설정 방법
1) 구독 내 액세스 제어(IAM) 선택


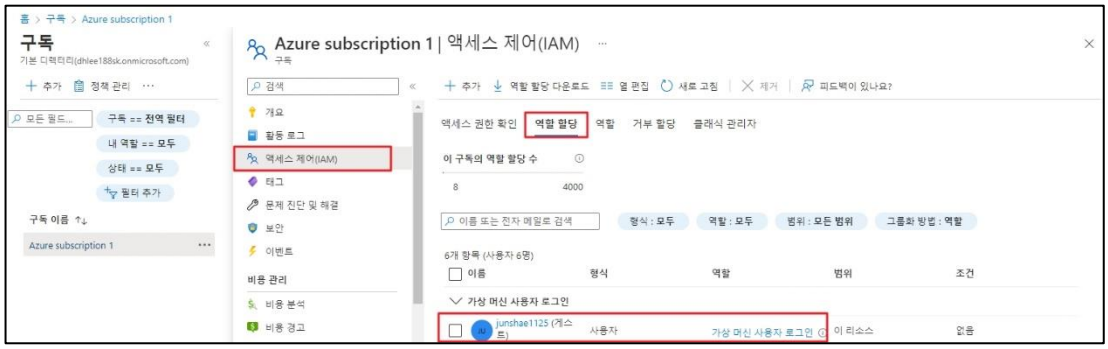
2) 액세스 제어(IAM) 선택 후 역할 할당 추가 버튼 클릭


</td></tr>
</table>

3) 추가할 역할 선택

4) 역할을 할당할 사용자 선택

5) 역할 할당 추가 검토/할당

	6) 액세스 제어(IAM) 내 역할 할당 메뉴에서 설정된 역할 및 계정 확인 
진단 기준	**양호기준** : 구독에 설정된 액세스 제어 역할이 서비스별 독자 권한(읽기)으로 부여되어 있는 경우 **취약기준** : 구독에 설정된 액세스 제어 역할에 전체 서비스 권한(소유자, 기여자, 사용자 액세스 관리자, 독자)으로 부여되어 있을 경우
비고	구독은 리소스 그룹의 최상위 리소스로 액세스 역할을 할당할 경우 구독 내 모든 리소스 그룹에 권한이 상속되기 때문에 구독은 최소한의 역할로 관리해야 하며, 리소스 그룹 내 사용하고자 하는 액세스 제어(IAM) 역할을 개별 설정하여 관리하여야 함

2.2 리소스 그룹 액세스 제어(IAM) 역할 할당

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">리소스 그룹 액세스 제어(IAM) 역할 할당</td></tr>
<tr><td>항목
설명</td><td colspan="3">
리소스 그룹은 Azure 솔루션에 관련된 리소스를 보유하는 컨테이너입니다. 리소스 그룹에는 솔루션에 대한 모든 리소스 또는 그룹으로 관리하려는 해당 리소스만 포함될 수 있습니다. 사용자의 조직에 가장 적합한 내용에 따라 리소스 그룹에 리소스를 어떻게 할당할지 결정합니다. 일반적으로 쉽게 배포, 업데이트하고 그룹으로 삭제할 수 있도록 동일한 리소스 그룹에 대해 동일한 수명 주기를 공유하는 리소스를 추가합니다.

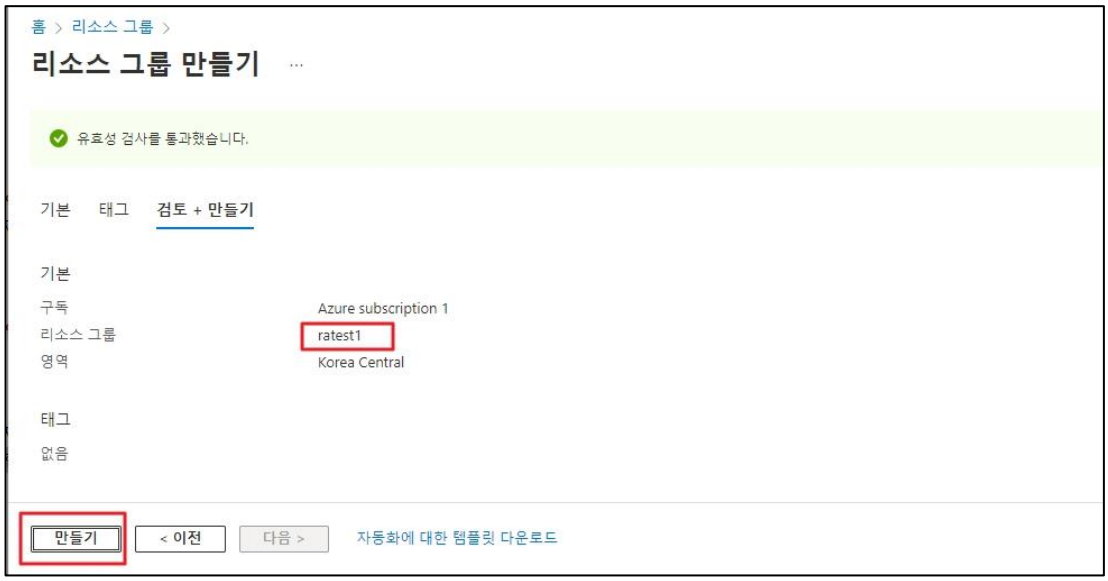
"소유자/기여자/사용자 액세스 관리자" 권한은 IAM 계정 역할 중 가능 높은 권한들로 클라우드 리소스에 대한 전반적인 작업을 가능하게 합니다. 이처럼 높은 권한은 최소한의 관리자에게만 부여되어야 하며, 인가되지 않거나 불필요한 계정에 부여되지 않도록 해야 합니다.

※ IAM 사용자 역할(예시)
<table>
<tr><th>역할 이름</th><th>역할 구분</th><th>상세설명</th></tr>
<tr><td>소유자</td><td>일반</td><td>Azure RBAC 에서 역할을 할당하는 기능을 포함하여 모든 리소스를 관리할 수 있는 모든 권한을 부여합니다.</td></tr>
<tr><td>기여자</td><td>일반</td><td>모든 리소스를 관리할 수 있는 모든 권한을 부여하지만 Azure RBAC 에서 역할 할당, Azure Blueprints 에서 할당 관리 또는 이미지 갤러리 공유를 허용하지 않습니다.</td></tr>
<tr><td>사용자 액세스 관리자</td><td>일반</td><td>Azure 리소스에 대한 사용자 액세스를 관리할 수 있음</td></tr>
<tr><td>독자</td><td>일반</td><td>모든 리소스를 볼 수 있지만 변경할 수는 없습니다.</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">
가. 리소스 그룹 생성
1) 리소스 그룹 추가


</td></tr>
</table>

2) 리소스 그룹 이름 설정

3) 리소스 그룹 만들기



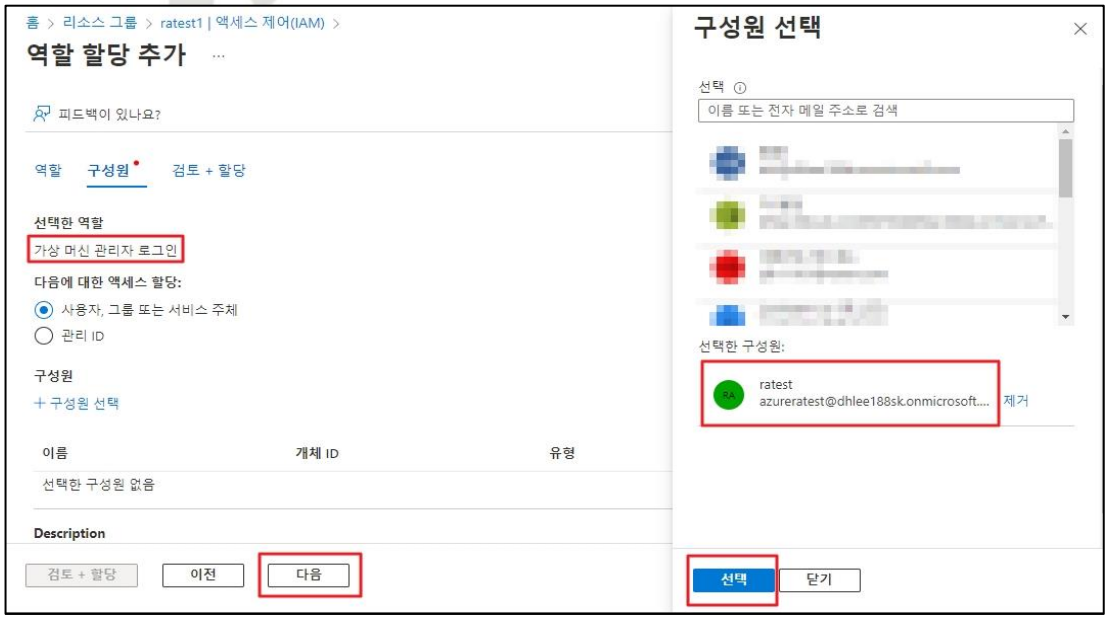
4) 리소스 그룹 생성 완료

나. 리소스 그룹 역할 설정

1) 리소스 그룹 역할 할당 추가

2) 사용하고자 하는 서비스에 대한 액세스 제어(IAM) 역할 추가

3) 역할 할당 구성원 선택



4) 역할 할당 추가 검토

5) 역할 할당 추가 완료 및 확인

진단 기준	**양호기준** : AZURE 사용자의 권한/그룹을 목적에 맞게 역할을 할당하고 있을 경우 **취약기준** : AZURE 사용자의 권한/그룹을 목적에 맞게 역할을 할당하고 있지 않을 경우
비고	

2.3 AD 사용자 역할 권한 관리

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">AD 사용자 역할 권한 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure AD(Active Directory)는 클라우드 환경에서 제공하는 디렉터리 서비스로 직원들이 로그인하여 리소스에 액세스할 수 있게 해주는 ID 및 액세스 관리 서비스입니다. 그 중 역할 및 관리자 기능은 Azure AD 및 기타 Microsoft 서비스에 대한 액세스 권한을 부여하는 데 사용할 수 있는 관리자 역할을 설정할 수 있어, 서비스 및 관리 목적에 맞게 역할을 할당해야 합니다.

※ Azure AD 관리 역할(예시)
<table>
<tr><th>역할 이름</th><th>상세설명</th></tr>
<tr><td>전역 관리자</td><td>Azure AD 및 Azure AD ID 를 사용하는 Microsoft 서비스의 모든 측면을 관리할 수 있습니다.</td></tr>
<tr><td>인증 관리자</td><td>관리 사용자가 아닌 사용자의 인증 메소드 정보를 보고, 설정하고, 재설정하기 위해 액세스할 수 있습니다.</td></tr>
<tr><td>인증 정책 관리자</td><td>인증 방법 정책, 테넌트 전체 MFA 설정, 암호 보호 정책 및 확인 가능한 자격 증명을 만들고 관리할 수 있습니다.</td></tr>
<tr><td>사용자 관리자</td><td>제한된 관리자의 암호 재설정을 비롯하여 사용자 및 그룹의 모든 측면을 관리할 수 있습니다.</td></tr>
<tr><td>암호 관리자</td><td>비관리자 및 암호 관리자의 암호를 재설정할 수 있습니다.</td></tr>
<tr><td>외부 ID 공급자 관리자</td><td>직접 페더레이션에 사용할 ID 공급자를 구성할 수 있습니다.</td></tr>
<tr><td>클라우드 디바이스 관리자</td><td>Azure AD 에서 디바이스를 관리하기 위한 액세스가 제한됩니다.</td></tr>
<tr><td>라이선스 관리자</td><td>사용자 및 그룹에 대한 제품 라이선스를 관리할 수 있습니다.</td></tr>
<tr><td>조건부 액세스 관리자</td><td>조건부 액세스 기능을 관리할 수 있습니다.</td></tr>
<tr><td>기술 지원팀 관리자</td><td>관리자가 아닌 관리자 및 기술 지원팀 관리자의 암호를 재설정할 수 있습니다.</td></tr>
<tr><td>서비스 지원 관리자</td><td>서비스 상태 정보를 읽고 지원 티켓을 관리할 수 있습니다.</td></tr>
<tr><td>애플리케이션 관리자</td><td>앱 등록 및 엔터프라이즈 앱의 모든 측면을 만들고 관리할 수 있습니다.</td></tr>
<tr><td>클라우드 애플리케이션 관리자</td><td>앱 프록시를 제외한 앱 등록 및 엔터프라이즈 앱의 모든 측면을 만들고 관리할 수 있습니다.</td></tr>
<tr><td>보안 관리자</td><td>Azure AD 및 Office 365 에서 보안 정보 및 보고서를 읽고 구성을 관리할 수 있습니다.</td></tr>
<tr><td>권한있는 역할 관리자</td><td>Azure AD 의 역할 할당 및 Privileged Identity Management 의 모든 측면을 관리할 수 있습니다.</td></tr>
<tr><td>권한있는 인증 관리자</td><td>사용자(관리자 또는 비관리자)의 인증 방법 정보를 보고, 설정하고. 재설정하기 위해 액세스할 수 있습니다.</td></tr>
</table></td></tr>
</table>

준수 관리자	Azure AD 및 Microsoft 365 준수 구성 및 보고서를 읽고 관리할 수 있습니다.
준수 데이터 관리자	준수 콘텐츠를 만들고 관리합니다.
데스크톱 분석 관리자	데스크톱 관리 도구 및 서비스에 액세스하고 관리할 수 있습니다.
Azure Information Protection 관리자	Azure Information Protection 제품의 모든 측면을 관리할 수 있습니다.

※ 관리자/운영자 접근 계정 운영대장(예시)

Cloud Admin Console 관리자 및 운영자 접근 계정 운영 대장							
No.	사용자 구분	사용자	부서명	직급	Cloud 접근 서비스	접근 목적	삭제 및 폐기일자
1	관리자	XXX	XXX팀	XX	ALL	Cloud 서비스 관리	20XX-XX-XX
2	운영자	XXX	XXX팀	XX	Monitoring / Backup	Cloud 서비스 운영	20XX-XX-XX
3	개발자	XXX	XXX팀	XX	DBMS Dev	WEB, DBMS 개발	20XX-XX-XX
4	비용집행자	XXX	XXX팀	XX	Cost Admin	서비스 비용 관리	20XX-XX-XX
(*) 관리자, 운영자, 개발자, 비용처리자 계정은 타인에게 양도 할 수 없고, 1인 1계정으로 활용되어야 함 관리 및 특수 권한 계정 사용자가 퇴직할 경우 더 이상 사용할 수 없도록 삭제하거나 비활성화해야 함							

설정 방법

가. Active Directory 사용자 권한 확인

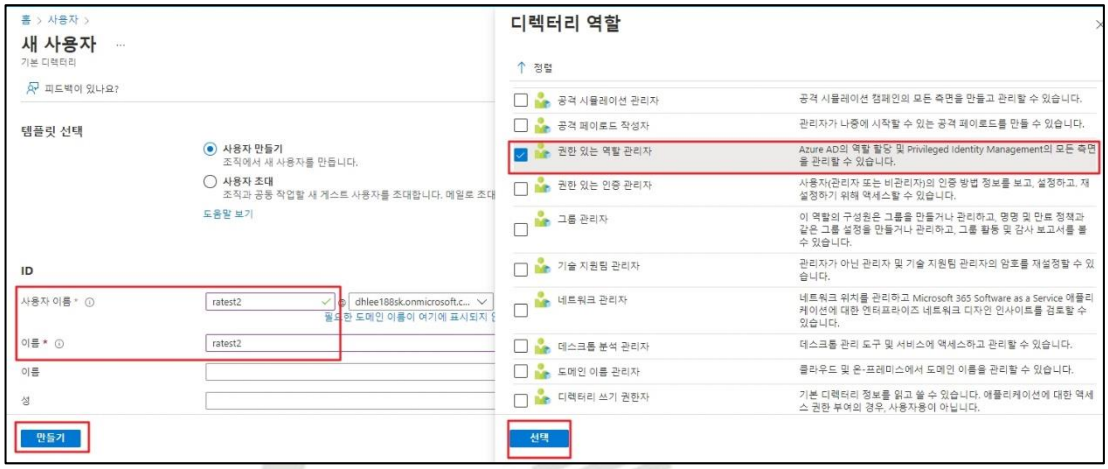
1) Active Directory 사용자 목록 확인

2) Active Directory 사용자의 할당된 역할 확인

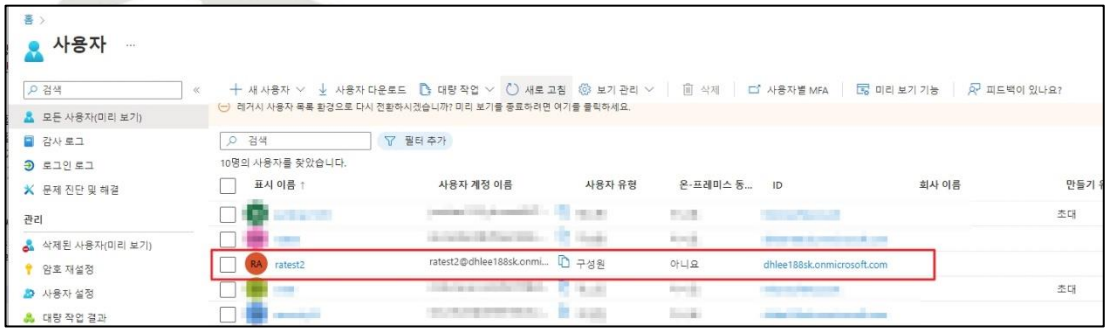
나. Active Directory 사용자 생성 및 관리자 권한 부여

1) 새 사용자 추가

2) 계정 정보 입력 및 서비스 목적에 맞는 관리자 역할 할당



3) 사용자 추가 확인



4) 사용자에 할당된 역할 확인

진단 기준	**양호기준** : AD 관리 역할이 업무 및 서비스 사용 목적에 맞게 부여되어 있을 경우 **취약기준** : AD 관리 역할이 업무 및 서비스 사용 목적에 맞게 부여되어 있지 않을 경우
비고	

2.4 인스턴스 서비스 액세스 정책 관리

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">인스턴스 서비스 액세스 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure RBAC(Azure 역할 기반 액세스 제어)를 사용하면 팀 내에서 업무를 분리하고 인스턴스 서비스(가상 머신, Container Instances, Kubernetes Services 등)에서 사용자에게 해당 작업을 수행하는 데 필요한 만큼의 권한만 부여할 수 있습니다. 인스턴스 서비스에서 모든 사람에게 무제한 권한을 제공하는 대신 특정 작업만 허용할 수 있습니다.

※ 인스턴스 서비스 예시
<table>
<tr><th>서비스명</th><th>상세설명</th></tr>
<tr><td>가상머신</td><td>Azure VMs 는 Azure 에서 제공하는 여러 유형의 확장 가능한 주문형 컴퓨팅 리소스 중 하나입니다. VMs 를 사용하면 구성을 완벽하게 제어할 수 있으며, 작업을 수행하는 데 필요한 모든 요소를 설치할 수 있습니다.</td></tr>
<tr><td>Container Instances</td><td>Azure Container Instances 는 오케스트레이션 없이 격리된 컨테이너에서 작동할 수 있는 모든 시나리오에 대한 솔루션입니다. 이벤트 기반 애플리케이션을 실행하고, 컨테이너 개발 파이프라인에서 신속하게 배포하고, 데이터 처리 및 빌드 작업을 실행합니다.</td></tr>
<tr><td>Kubernates</td><td>AKS(Azure Kubernetes Service)는 운영 오버헤드를 Azure 로 오프로드하여 Azure 에서 관리되는 Kubernetes 클러스터 배포를 단순화합니다. 호스팅되는 Kubernetes 서비스인 Azure 는 상태 모니터링 및 유지 관리 같은 중요 작업을 처리합니다.</td></tr>
<tr><td>스토리지 계정</td><td>스토리지 계정은 HTTP 또는 HTTPS 를 통해 전 세계 어디에서나 액세스할 수 있는 Azure Storage 데이터에 고유한 네임스페이스를 제공합니다. 스토리지 계정의 데이터는 지속적이고 가용성이 높으며 안전하고 대규모로 확장 가능합니다.</td></tr>
<tr><td>Data Lake Storage</td><td>Azure Data Lake Storage 가 가용성, 보안, 내구성, 확장성 및 중복성이 뛰어난 클라우드 스토리지 서비스를 제공하고, 빅 데이터 분석 워크로드를 처리하는 데 새로운 효율성을 제공하는 서비스입니다.</td></tr>
<tr><td>Cosmos DB</td><td>완전 관리형 서비스인 Azure Cosmos DB 는 자동 관리, 업데이트 및 패치를 통해 데이터베이스 관리를 직접 수행할 수 있습니다. 또한 용량과 비용을 일치시키기 위해 애플리케이션 요구 사항에 대응하는 비용 효율적인 서버 리스 및 자동 확장 옵션으로 용량 관리를 처리합니다.</td></tr>
</table>
</td></tr>
</table>

SQL Database	Azure SQL Database 는 사용자 개입 없이 업그레이드, 패치, 백업, 모니터링 같은 대부분의 데이터베이스 관리 기능을 처리하는 완전 관리형 PaaS(Platform as a Service) 데이터베이스 엔진입니다.
Database MySQL	Azure Database for MySQL 은 MySQL 커뮤니티 버전(GPLv2 라이선스에서 사용 가능) 데이터베이스 엔진, 버전 5.6(사용 중지됨), 5.7 및 8.0 을 기준으로 하는 Microsoft 클라우드의 관계형 데이터베이스 서비스입니다. MySQL 용 Azure Database 는 다음과 같은 기능을 제공합니다.

※ 인스턴스 서비스 액세스 제어(IAM) 역할(예시)

역할 이름	역할 구분	상세설명
AcrPull	컨테이너	acr 끌어오기
AcrPush	컨테이너	acr 푸시
AcrDelete	컨테이너	ACR 삭제
Avere 연산자	스토리지	Avere vFXT 클러스터에서 클러스터를 관리하는 데 사용됩니다.
Avere 참가자	스토리지	Avere vFXT 클러스터를 만들고 관리할 수 있습니다.
Azure Kubernetes Service RBAC 관리자	컨테이너	리소스 할당량 및 네임스페이스 업데이트 또는 삭제를 제외하고 클러스터/네임스페이스의 모든 리소스를 관리할 수 있습니다.
Azure Kubernetes Service RBAC 클러스터 관리자	컨테이너	클러스터의 모든 리소스를 관리할 수 있습니다.
Azure Kubernetes Service RBAC 쓰기 권한자	컨테이너	네임스페이스에 있는 대부분의 개체에 대한 읽기/쓰기 권한을 허용합니다. 해당 역할은 역할 또는 역할 바인딩을 보거나 수정할 수 없습니다.
Azure Kubernetes Service RBAC 읽기 권한자	컨테이너	네임스페이스에 있는 대부분의 개체를 볼 수 있는 읽기 전용 권한을 허용합니다. 역할 또는 역할 바인딩을 볼 수는 없습니다.
Azure Kubernetes Service 기여자 역할	컨테이너	클러스터 관리 자격 증명 작업을 나열합니다.
Azure Kubernetes Service 클러스터 관리 역할	컨테이너	클러스터 관리 자격 증명 작업을 나열합니다.
Azure Kubernetes Service 클러스터 사용자 역할	컨테이너	클러스터 사용자 자격 증명 작업을 나열합니다.

Cosmos DB 계정 독자 역할	데이터베이스	Azure Cosmos DB 계정 데이터를 읽을 수 있음
Cosmos DB 연산자	데이터베이스	Azure Cosmos DB 계정을 관리할 수 있지만 데이터에 액세스할 수는 없습니다. 계정 키 및 연결 문자열에 대한 액세스를 차단합니다.
CosmosBackupOperator	데이터베이스	Cosmos DB 데이터베이스 또는 계정의 컨테이너에 대해 복구 요청을 제출할 수 있습니다.
CosmosRestoreOperator	데이터베이스	지속적인 백업 모드를 사용하여 Cosmos DB 데이터베이스 계정의 복원 작업을 수행할 수 있습니다.
Data Box 참가자	스토리지	다른 사용자에게 액세스 권한을 부여하는 기능을 제외한 Data Box Service 의 모든 기능을 관리할 수 있습니다.
Data Box 판독기	스토리지	주문을 작성하거나 주문 정보를 편집하고 다른 사용자에게 액세스 권한을 부여하는 기능을 제외한 Data Box Service 를 관리할 수 있습니다.
Data Lake Analytics 개발자	스토리지	사용자 자신의 작업을 제출, 모니터링 및 관리할 수 있지만 Data Lake Analytics 계정을 만들거나 삭제할 수는 없습니다.
DocumentDB 계정 참가자	데이터베이스	DocumentDB 계정을 관리할 수 있지만 액세스할 수는 없습니다.
Redis Cache 참가자	데이터베이스	Redis Cache 를 관리할 수 있지만 액세스할 수는 없습니다.
SQL 보안 관리자	데이터베이스	SQL Server 및 데이터베이스의 보안과 관련된 정책을 관리할 수 있지만 여기에 액세스할 수는 없습니다.
SQL Managed Instance Contributor	데이터베이스	SQL Managed Instances 및 필수 네트워크 구성을 관리할 수 있지만 다른 사용자에게 액세스 권한을 부여할 수 없습니다.
SQL Server 참가자	데이터베이스	SQL Server 및 데이터베이스를 관리할 수 있지만 여기에 액세스할 수는 없으며, 해당하는 보안과 관련된 정책에도 액세스할 수 없습니다.
SQL DB 참가자	데이터베이스	SQL 데이터베이스를 관리할 수 있지만 액세스할 수는 없으며, SQL 데이터베이스의 보안 관련 정책 또는 부모 SQL 서버도 관리할 수 없습니다.
Storage Blob 데이터 Contributor	스토리지	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage Blob 데이터 Reader	스토리지	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기 액세스를 허용

Storage Blob 데이터 소유자	스토리지	POSIX 액세스 제어 할당을 포함하여 Azure Storage Blob 컨테이너 및 데이터에 대한 모든 권한을 허용합니다.
Storage Blob 위임자	스토리지	SAS 토큰에 서명하는 데 사용할 수 있는 사용자 위임 키를 생성하도록 허용합니다.
Storage 계정 참가자	스토리지	스토리지 계정 데이터에 대한 전체 액세스를 스토리지 저장소 계정 키 액세스를 포함하여 스토리지 계정을 관리할 수 있습니다.
Storage 큐 데이터 Contributor	스토리지	Azure Storage 큐 및 큐 메시지에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage 큐 데이터 Reader	스토리지	Azure Storage 큐 및 큐 메시지에 대한 읽기 액세스를 허용
Storage 큐 데이터 메시지 보낸 사람	스토리지	Azure Storage 큐 메시지 보내기 허용
Storage 큐 데이터 메시지 프로세서	스토리지	Azure Storage 큐 메시지에 대한 미리 보기, 수신 및 삭제 권한 허용
가상 머신 관리자 로그인	컴퓨팅	포털에서 가상 머신을 보고 관리자로 로그인
가상 머신 사용자 로그인	컴퓨팅	포털에서 가상 머신을 보고 일반 사용자로 로그인합니다.
가상 머신 참가자	컴퓨팅	가상 컴퓨터를 관리할 수 있지만 가상 컴퓨터나 가상 컴퓨터가 연결된 가상 네트워크 또는 저장소 계정에 액세스할 수는 없습니다.
백업 운영자	스토리지	백업 제거를 제외한 백업 서비스를 관리하고 자격 증명 모음 만들고 다른 사람에게 액세스 권한을 부여할 수 있습니다.
백업 참가자	스토리지	백업 서비스를 관리할 수 있지만, 자격 증명 모음을 만들고 다른 사용자에게 액세스 권한을 부여할 수는 없습니다.
백업 독자	스토리지	백업 서비스를 볼 수 있지만 변경할 수는 없습니다.
스토리지 계정 키 운영자 서비스 역할	스토리지	스토리지 계정 키 운영자가 스토리지 계정에서 키를 나열하고 다시 생성할 수 있습니다.
스토리지 계정 백업 기여자 역할	스토리지	스토리지 계정 백업 기여자는 스토리지 계정의 백업 및 복원을 수행할 수 있습니다.
스토리지 테이블 데이터 읽기 권한자	스토리지	Azure Storage 테이블 및 엔터티에 대한 읽기 액세스 허용
스토리지 파일 데이터 SMB 공유 상승된 기여자	스토리지	SMB 를 통해 Azure Storage 파일 공유에서 읽기, 쓰기, 삭제 및 NTFS 권한 수정 허용

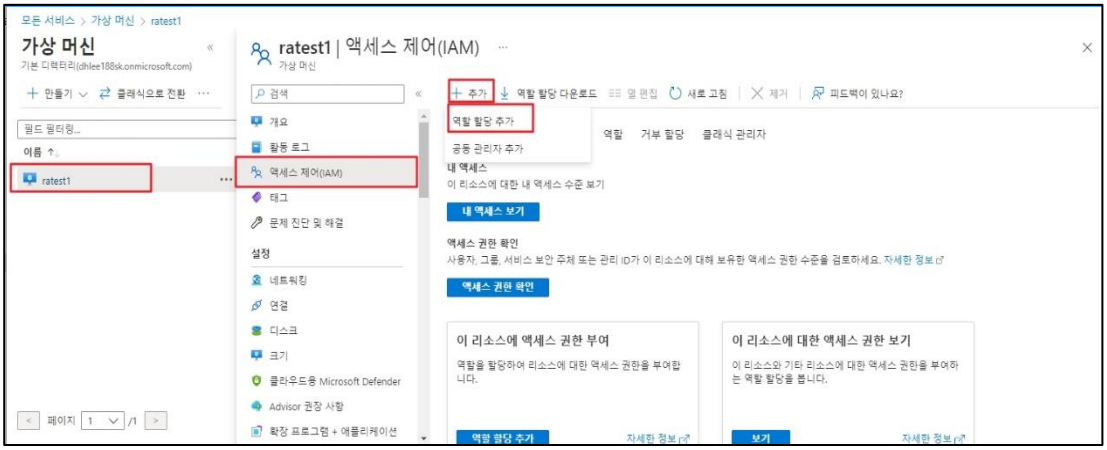
스토리지 파일 데이터 SMB 공유 읽기 권한자	스토리지	SMB 를 통해 Azure 파일 공유에 대한 읽기 액세스 허용
스토리지 파일 데이터 SMB 공유 참가자	스토리지	SMB 를 통해 Azure Storage 파일 공유에서 읽기, 쓰기 및 삭제 액세스 허용
읽기 권한자 및 데이터 액세스	스토리지	모든 항목을 볼 수 있지만, 스토리지 계정 또는 포함된 리소스를 삭제하거나 만들 수는 없습니다.
저장소 테이블 데이터 기여자	스토리지	Azure Storage 테이블 및 엔터티에 대한 읽기, 쓰기 및 삭제 액세스 허용
클래식 Storage 계정 참가자	스토리지	클래식 Storage 계정을 관리할 수 있지만 여기에 액세스할 수는 없습니다.
클래식 가상 머신 참가자	컴퓨팅	클래식 가상 머신을 관리할 수 있지만 가상 머신이나 연결된 가상 네트워크 또는 스토리지 계정에 액세스할 수는 없습니다.
클래식 스토리지 계정 키 운영자 서비스 역할	스토리지	클래식 스토리지 계정 키 운영자가 클래식 스토리지 계정에서 키를 나열하고 다시 생성할 수 있습니다.

설정 방법

가. 인스턴스 서비스 액세스 제어(IAM) 추가

1) 인스턴스 서비스(가상머신) 목록 확인

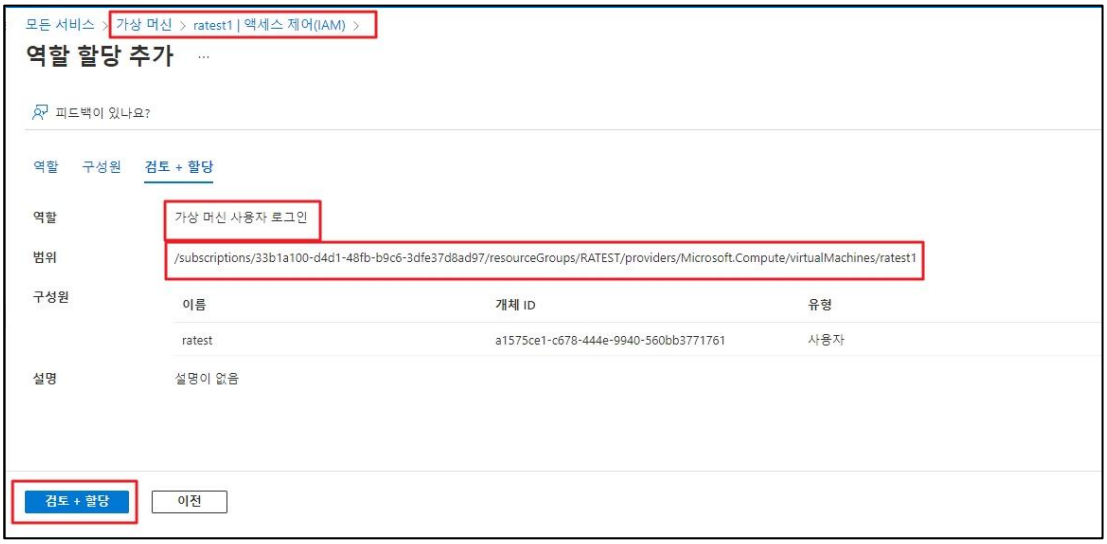
2) 인스턴스 내 IAM 역할 할당 추가

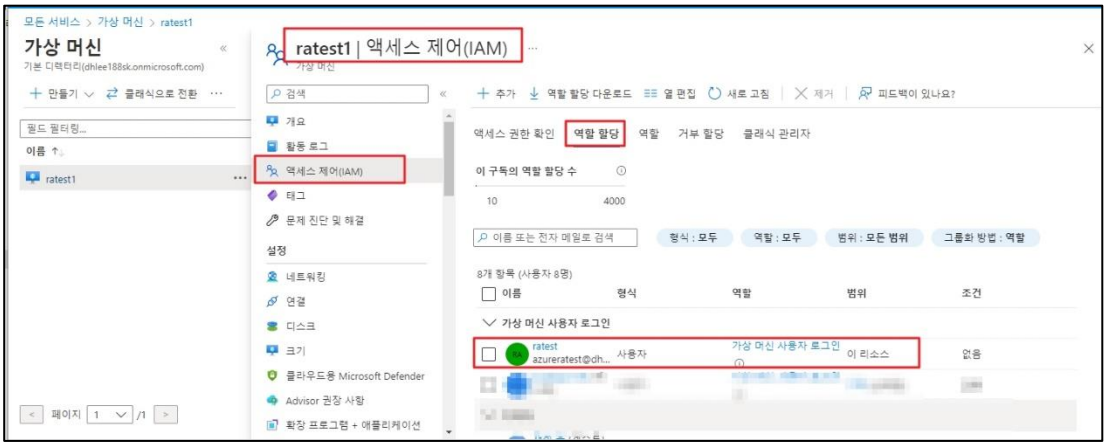


3) 서비스 목적에 맞는 역할 할당 추가

4) 역할 할당 구성원 추가

5) 역할 할당 검토



	6) 역할 할당 추가 완료 및 확인 
진단 기준	**양호기준** : 인스턴스 서비스에 대한 액세스 제어(IAM)가 사용자 역할에 맞게 부여되어 있는 경우 **취약기준** : 인스턴스 서비스에 대한 액세스 제어(IAM)가 사용자 역할에 맞게 부여되어 있지 않은 경우
비고	

2.5 네트워크 서비스 액세스 정책 관리

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">네트워크 서비스 액세스 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure RBAC(Azure 역할 기반 액세스 제어)를 사용하면 팀 내에서 업무를 분리하고 네트워크 서비스(가상 네트워크, Front Door 및 CDN 프로필, 가상 네트워크 게이트 웨이 등)에서 사용자에게 해당 작업을 수행하는 데 필요한 만큼의 권한만 부여할 수 있습니다. 네트워크 서비스에서 모든 사람에게 무제한 권한을 제공하는 대신 특정 작업만 허용할 수 있습니다.

※ 네트워크 서비스 예시
<table>
<tr><th>서비스명</th><th>상세설명</th></tr>
<tr><td>가상네트워크</td><td>Azure Virtual Network(VNet)는 Azure 의 프라이빗 네트워크의 기본 구성 요소입니다. VNet 을 사용하면 Azure VM(Virtual Machines)과 같은 다양한 형식의 Azure 리소스가 서로, 인터넷 및 특정 온-프레미스 네트워크와 안전하게 통신할 수 있습니다.</td></tr>
<tr><td>Front Door 및 CDN 프로필</td><td>Azure Front Door 는 전 세계 사용자와 애플리케이션의 정적 및 동적 웹 콘텐츠 간에 빠르고 안정적이며 안전한 액세스를 제공하는 Microsoft 의 CDN(Content Delivery Network) 서비스 입니다</td></tr>
<tr><td>프라이빗 링크 허브</td><td>Azure Private Link 를 사용하면 가상 네트워크의 프라이빗 엔드포인트를 통해 Azure PaaS Services(예: Azure Storage 및 SQL Database)와 Azure 호스팅 고객 소유/파트너 서비스에 액세스할 수 있습니다.</td></tr>
<tr><td>네트워크 보안 그룹</td><td>네트워크 보안 그룹은 Azure 구독 제한 내에서 필요한 만큼 0 개 또는 많은 규칙을 포함하며 네트워크 보안 그룹을 사용하여 Azure 가상 네트워크의 Azure 리소스 간의 네트워크 트래픽을 필터링할 수 있습니다. 네트워크 보안 그룹에는 여러 종류의 Azure 리소스에서 오는 인바운드 트래픽 또는 이러한 리소스로 나가는 아웃바운드 네트워크 트래픽을 허용하거나 거부하는 보안 규칙이 포함됩니다. 규칙마다 원본 및 대상, 포트, 프로토콜을 지정할 수 있습니다.</td></tr>
<tr><td>공용 IP 주소</td><td>공용 IP 주소를 통해 인터넷 리소스가 Azure 리소스에 대한 인바운드와 통신할 수 있습니다. 공용 IP 를 사용하면 Azure 리소스에서 인터넷 및 공용 Azure 서비스에 통신할 수 있습니다. 주소는 사용자가 할당 해제하지 않는 한 리소스에 전용됩니다. 공용 IP 가 할당되지 않은 리소스는 아웃바운드로 통신할 수 있습니다.</td></tr>
<tr><td>경로 테이블</td><td>Azure 에서는 기본적으로 가상 네트워크 내의 모든 서브넷 간에 트래픽을 라우팅합니다. 고유의 라우팅을 만들어 Azure 의 기본 라우팅을 재정의할 수 있습니다. 예를 들어, NVA(네트워크 가상 어플라이언스)를 통해 트래픽을 서브넷 간에 라우팅하려는 경우, 사용자 지정 경로가 유용합니다.</td></tr>
</table>
</td></tr>
</table>

애플리케이션 보안그룹	애플리케이션 보안 그룹을 선택하는 경우 기존 애플리케이션 보안 그룹도 선택해야 합니다. 원본 및 대상 둘 다에 대해 애플리케이션 보안 그룹을 선택하는 경우 두 애플리케이션 보안 그룹 내 네트워크 인터페이스가 동일한 가상 네트워크에 있어야 합니다.
DNS 영역	DNS 영역은 특정 도메인에 대한 DNS 레코드를 호스트하는 데 사용됩니다. Azure DNS 에서 도메인 호스팅을 시작하려면 해당 도메인 이름의 DNS 영역을 만들어야 합니다. 그러면 이 DNS 영역 안에 도메인의 각 DNS 레코드가 생성됩니다.
NAT 게이트웨이	Virtual Network NAT 는 완전 관리되고 복원력이 뛰어난 NAT(네트워크 주소 변환) 서비스입니다. Virtual Network NAT 는 Virtual Network 에 대한 아웃바운드 인터넷 연결을 단순화합니다. 서브넷에 구성된 경우 모든 아웃바운드 연결은 Virtual Network NAT 의 고정 공용 IP 주소를 사용합니다.
가상 네트워크 게이트웨이	퍼블릭 인터넷을 통해 Azure 가상 네트워크와 온-프레미스 위치 간의 트래픽을 전송하는 데 사용되는 특정 유형의 가상 네트워크 게이트웨이입니다
애플리케이션 게이트웨이	Azure Application Gateway 는 웹 애플리케이션에 대한 트래픽을 관리할 수 있도록 하는 웹 트래픽 부하 분산 장치입니다. 기존 부하 분산 장치는 전송 계층(OSI 계층 4 - TCP 및 UDP)에서 작동하고 원본 IP 주소와 포트를 기반으로 대상 IP 주소와 포트에 트래픽을 라우팅합니다.

※ 네트워크 서비스 액세스 제어(IAM) 역할(예시)

역할 이름	역할 구분	상세설명
CDN 엔드포인트 독자	네트워킹	CDN 엔드포인트를 볼 수 있지만 변경할 수는 없습니다.
CDN 엔드포인트 참가자	네트워킹	CDN 엔드포인트를 관리할 수 있지만 다른 사용자에게 액세스 권한을 부여할 수는 없습니다.
CDN 프로필 독자	네트워킹	CDN 프로필과 해당 엔드포인트를 볼 수 있지만 변경할 수는 없습니다.
CDN 프로필 참가자	네트워킹	CDN 프로필과 해당 엔드포인트를 관리할 수 있지만 다른 사용자에게 액세스 권한을 부여할 수는 없습니다.
DNS Resolver Contributor	네트워킹	DNS 확인자 리소스를 관리할 수 있습니다.
DNS 영역 참가자	네트워킹	Azure DNS 의 DNS 영역과 레코드 집합을 관리할 수 있지만 액세스할 수 있는 사람을 제어할 수는 없습니다.
네트워크 참가자	네트워킹	네트워크를 관리할 수 있지만 액세스할 수는 없습니다.

클래식 네트워크 참가자	네트워킹	기본 네트워크를 관리할 수 있지만 액세스할 수는 없습니다.
프라이빗 DNS 영역 참가자	네트워킹	프라이빗 DNS 영역 리소스는 관리할 수 있으나, 연결되어 있는 가상 네트워크는 관리할 수 없습니다.

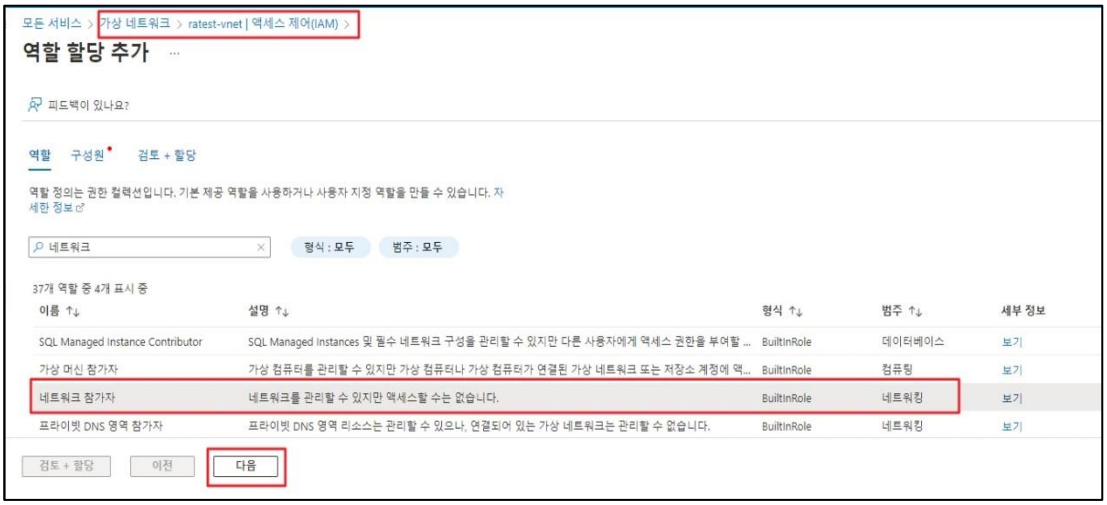
설정 방법

가. 네트워크 서비스 액세스 제어(IAM) 추가

1) 네트워크 서비스(가상 네트워크) 목록 확인

2) 가상 네트워크 내 IAM 역할 할당 추가

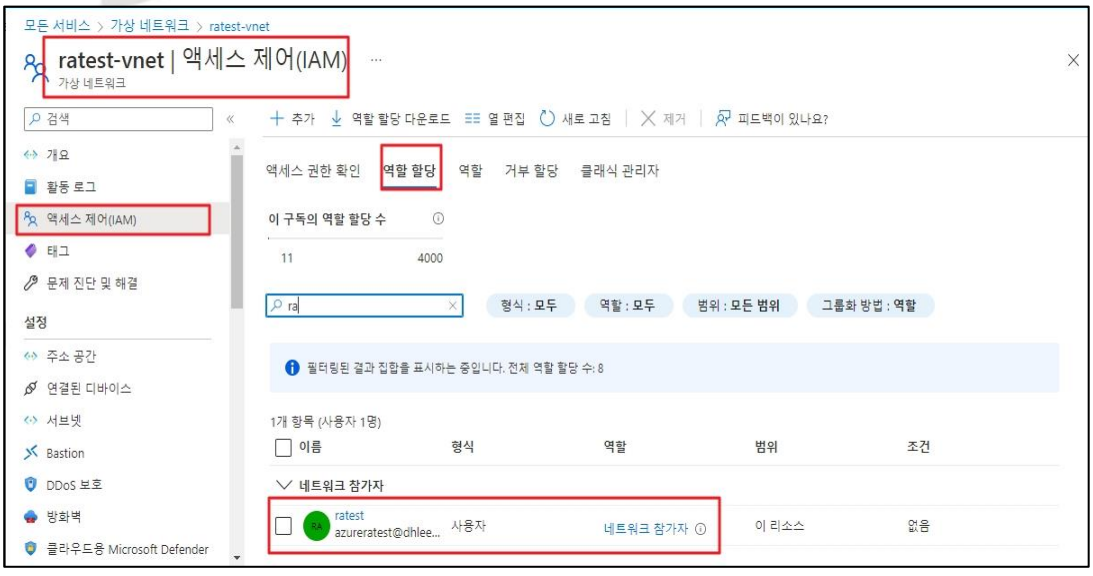
3) 서비스 목적에 맞는 역할 할당 추가



4) 역할 할당 구성원 추가

5) 역할 할당 검토

6) 역할 할당 추가 완료 및 확인



진단 기준	**양호기준** : 네트워크 서비스에 대한 액세스 제어(IAM)가 사용자 역할에 맞게 부여되어 있는 경우 **취약기준** : 네트워크 서비스에 대한 액세스 제어(IAM)가 사용자 역할에 맞게 부여되어 있지 않은 경우
비고	

2.6 기타 서비스 액세스 정책 관리

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">인스턴스 서비스 액세스 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure RBAC(Azure 역할 기반 액세스 제어)를 사용하면 팀 내에서 업무를 분리하고 기타 서비스(Azure Active Directory, 모니터, 키 자격 증명 모음 등)에서 사용자에게 해당 작업을 수행하는 데 필요한 만큼의 권한만 부여할 수 있습니다. 기타 서비스에서 모든 사람에게 무제한 권한을 제공하는 대신 특정 작업만 허용할 수 있습니다.

※ 기타 서비스 예시
<table>
<tr><th>서비스명</th><th>상세설명</th></tr>
<tr><td>Virtual Machine Scale Sets</td><td>Azure Virtual Machine Scale Sets 많은 VM 에서 실행되는 애플리케이션에 대한 관리 기능, 리소스의 자동 크기 조정 및 트래픽 부하 분산을 제공합니다. 확장 집합에서 제공하는 주요 이점은 다음과 같습니다.</td></tr>
<tr><td>부하 분산 장치</td><td>Azure Load Balancer 는 계층 4 네트워크 부하 분산 장치입니다. 옵션은 TCP 또는 UDP 입니다. 이 설정은 부하 분산 규칙에 따라 트래픽을 배포할 프런트 엔드 IP 와 연결된 포트입니다. 이 설정은 부하 분산 장치에서 트래픽을 전송할 백 엔드 풀의 인스턴스 포트입니다.</td></tr>
<tr><td>WAF</td><td>Azure WAF 란? Azure WAF 는 SQL 삽입, 사이트 간 스크립팅 및 기타 웹 공격과 같은 일반적인 위협으로부터 웹 애플리케이션을 보호하는 데 유용한 웹 애플리케이션 방화벽입니다.</td></tr>
<tr><td>방화벽</td><td>Azure Firewall 은 Azure 에서 실행되는 클라우드 워크로드에 대해 최상의 위협 보호를 제공하는 클라우드 네이티브 및 지능형 네트워크 방화벽 보안 서비스입니다. 고가용성 및 무제한 클라우드 확장성이 기본 제공되는 서비스 형태의 완전한 상태 저장 방화벽입니다.</td></tr>
<tr><td>App Service</td><td>Azure App Service 는 웹 애플리케이션, REST API 및 모바일 백 엔드를 호스트하는 HTTP 기반 서비스입니다. .NET, .NET Core, Java, Ruby, Node.js, PHP 또는 Python 등 원하는 언어로 개발할 수 있습니다.</td></tr>
<tr><td>Data Lake Analytics</td><td>Azure Data Lake Analytics 는 빅 데이터를 간소화하는 주문형 분석 작업 서비스입니다. 하드웨어를 배포, 구성 및 조정하는 대신, 데이터를 변형하고 귀중한 통찰력을 얻기 위한 쿼리를 작성합니다.</td></tr>
<tr><td>Log Analytics</td><td>Log Analytics 는 Azure Monitor 로그에서 수집된 데이터에서 로그 쿼리를 편집 및 실행하고 그 결과를 대화형으로 분석하는 Azure Portal 의 도구입니다.</td></tr>
</table></td></tr>
</table>

Active Directory	Azure AD(Azure Active Directory)는 클라우드 기반 ID 및 액세스 관리 서비스입니다. 이 서비스를 통해 직원은 Microsoft 365, Azure Portal 및 수천 개의 기타 SaaS 애플리케이션과 같은 외부 리소스에 액세스할 수 있습니다. 또한 Azure Active Directory 는 조직용으로 개발된 클라우드 앱과 함께 회사 인트라넷 네트워크의 앱과 같은 내부 리소스에 액세스할 수 있도록 도와줍니다.
클라우드용 Microsoft Denfender	클라우드용 Microsoft Defender 는 모든 Azure, 온-프레미스 및 다중 클라우드(Amazon AWS 및 Google GCP) 리소스에 대한 CSPM(클라우드 보안 상태 관리) 및 CWPP(클라우드 워크로드 보호 플랫폼)입니다.
키 자격 증명 모음	Azure Key Vault 는 Azure 애플리케이션 및 사용자가 여러 가지 종류의 비밀/키 데이터를 저장하고 사용할 수 있는 서비스 입니다.
AD Identity Protection	Identity Protection 은 사용자 보호를 위해 Microsoft 가 Azure Active Directory 를 사용하는 조직, Microsoft 계정의 소비자 공간 및 Xbox 를 이용한 게임 등에서 사용자 위치로부터 습득한 학습을 사용합니다.
모니터	Azure Monitor 는 Azure 리소스를 모니터링하는 전체 기능 집합을 제공하는 전체 스택 모니터링 서비스입니다. Azure Monitor 를 사용하여 다른 클라우드 및 온-프레미스의 리소스를 모니터링할 수도 있습니다.
활동로그	Azure Monitor 활동 로그는 구독 수준 이벤트에 대한 정보를 제공하는 Azure 의 플랫폼 로그입니다. 활동 로그에는 리소스가 수정되거나 가상 머신이 시작될 때와 같은 정보가 포함됩니다.
Network Watcher	Azure Network Watcher 는 Azure 가상 네트워크의 리소스를 모니터링 및 진단하고 메트릭을 보고 그에 대한 로그를 활성화 또는 비활성화하는 도구를 제공합니다.
백업센터	백업 센터는 엔터프라이즈가 대규모 백업을 제어, 모니터링, 운영 및 분석할 수 있도록 Azure 에서 단일 통합 관리 환경을 제공합니다. 따라서 Azure 의 네이티브 관리 환경과 일치합니다.

※ 기타 서비스 액세스 제어(IAM) 역할(예시)

역할 이름	역할 구분	상세설명
API Management 참가자	통합	서비스 및 API 를 관리할 수 있습니다.
API Management 서비스 연산자 역할	통합	서비스를 관리할 수 있지만 API 는 관리할 수 없습니다.
API Management 서비스 독자 역할	통합	서비스 및 API 에 대한 읽기 전용 액세스

App Configuration 데이터 소유자	통합	App Configuration 데이터에 대한 모든 액세스 권한을 허용합니다.
App Configuration 데이터 읽기 권한자	통합	App Configuration 데이터에 대한 읽기 권한을 허용합니다.
Application Insights 구성 요소 참가자	모니터	Application Insights 구성 요소를 관리할 수 있습니다.
Application Insights 스냅샷 디버거	모니터	사용자에게 Application Insights 스냅샷 디버거 기능을 사용할 수 있는 권한을 부여합니다.
Automation Runbook 연산자	관리+거버넌스	Runbook 의 작업을 만들 수 있으려면 Runbook 속성을 읽으세요.
Automation 작업 연산자	관리+거버넌스	Automation Runbook 을 사용하여 작업을 만들고 관리합니다.
Azure Arc Kubernetes 관리자	관리+거버넌스	리소스 할당량 및 네임스페이스 업데이트 또는 삭제를 제외하고 클러스터/네임스페이스의 모든 리소스를 관리할 수 있습니다.
Azure Arc Kubernetes 클러스터 관리자	관리+거버넌스	클러스터의 모든 리소스를 관리할 수 있습니다.
Azure Arc Kubernetes 쓰기 권한자	관리+거버넌스	(클러스터)역할 및 (클러스터)역할 바인딩을 제외하고 클러스터/네임스페이스의 모든 항목을 업데이트할 수 있습니다.
Azure Arc Kubernetes 뷰어	관리+거버넌스	비밀을 제외하고 클러스터/네임스페이스의 모든 리소스를 볼 수 있습니다.
Azure Arc 사용 Kubernetes 클러스터 사용자 역할	관리+거버넌스	클러스터 사용자 자격 증명 작업을 나열합니다.
Azure Connected Machine 리소스 관리자	관리+거버넌스	Azure Connected Machines 을 읽고, 쓰고, 삭제하고, 다시 온보딩할 수 있습니다.
Azure Connected Machine 온보딩	관리+거버넌스	Azure Connected Machines 을 온보딩할 수 있습니다.
Azure Event Hubs 데이터 소유자	분석	Azure Event Hubs 리소스에 대한 전체 액세스를 허용합니다.
Azure Event Hubs 데이터 보낸 사람	분석	Azure Event Hubs 리소스에 대한 액세스 권한을 보낼 수 있습니다.
Azure Event Hubs 데이터 받는 사람	분석	Azure Event Hubs 리소스에 대한 액세스 권한을 받을 수 있습니다.
Cost Management 참가자	관리+거버넌스	비용을 확인하고 비용 구성(예: 예산, 내보내기)을 관리할 수 있습니다.

Cost Management 판독기	관리+거버넌스	비용 데이터 및 구성(예: 예산, 내보내기)을 볼 수 있습니다.
Data Factory 참가자	분석	데이터 팩터리를 만들고 관리하며 해당 하위 리소스도 만들고 관리합니다.
Domain Services Contributor	ID	Azure AD 도메인 서비스 및 관련 네트워크 구성을 관리할 수 있습니다.
Domain Services Reader	ID	Azure AD 도메인 서비스 및 관련 네트워크 구성을 볼 수 있습니다.
EventGrid 기여자	통합	EventGrid 작업을 관리할 수 있습니다.
EventGrid EventSubscription Contributor	통합	EventGrid 이벤트 구독 작업을 관리할 수 있습니다.
EventGrid EventSubscription Reader	통합	EventGrid 이벤트 구독을 읽을 수 있습니다.
HDInsight 도메인 서비스 참가자	분석	HDInsight Enterprise Security Package 에 필요한 도메인 서비스 관련 작업을 읽고, 작성하고, 수정하고 삭제할 수 있습니다.
HDInsight 클러스터 연산자	분석	HDInsight 클러스터 구성을 읽고 수정할 수 있습니다.
Key Vault 관리자	보안	키 자격 증명 모음과 인증서, 키, 비밀 등 모음 내의 모든 개체에 대한 모든 데이터 평면 작업을 수행합니다.
Key Vault 비밀 책임자	보안	사용 권한 관리를 제외하고 키 자격 증명 모음의 비밀에 대한 모든 작업을 수행합니다.
Key Vault 비밀 사용자	보안	비밀 내용을 읽습니다. 'Azure 역할 기반 액세스 제어' 권한 모델을 사용하는 키 자격 증명 모음에만 적용됩니다.
Key Vault 암호화 책임자	보안	사용 권한 관리를 제외하고 키 자격 증명 모음의 키에 대한 모든 작업을 수행합니다.
Key Vault 인증서 책임자	보안	사용 권한 관리를 제외하고 키 자격 증명 모음의 인증서에 대한 모든 작업을 수행합니다.
Key Vault 암호화 서비스 암호화 사용자	보안	키의 메타데이터를 읽고 래핑/래핑 해제 작업을 수행합니다.
Key Vault 암호화 사용자	보안	키를 사용하여 암호화 작업을 수행합니다.
Key Vault 읽기 권한자	보안	키 자격 증명 모음과 해당 인증서, 키 및 비밀의 메타데이터를 읽습니다.

Key Vault 참가자	보안	Key Vault 를 관리할 수 있지만 액세스할 수는 없습니다.
Kubernetes 확장 참가자	관리+거버넌스	Kubernetes 확장을 만들고, 업데이트하고, 가져오고, 나열 및 삭제하고, 확장 비동기 작업을 가져올 수 있습니다.
Kubernetes 클러스터 - Azure Arc 온보딩	관리+거버넌스	ConnectedClusters 리소스를 만들기 위해 모든 사용자/서비스에 권한을 부여하는 역할 정의
Log Analytics 독자	분석	Log Analytics 독자는 모든 Azure 리소스에 대한 Azure Diagnostics 의 구성 보기를 비롯하여 모니터링 설정 보기 및 모든 모니터링 데이터를 보고 검색할 수 있습니다.
Log Analytics 참가자	분석	og Analytics 기여자는 모든 모니터링 데이터를 읽고 모니터링 설정을 편집할 수 있습니다.
Logic Apps 연산자	통합	Logic Apps 을 읽을 수 있으며 사용하거나 사용하지 않도록 설정할 수 있습니다.
Logic Apps 참가자	통합	Logic Apps 을 관리할 수 있지만 여기에 액세스할 수는 없습니다.
Media Services 계정 관리자	웹	Media Services 계정 생성, 읽기, 수정 및 삭제, 다른 Media Services 리소스에 대한 읽기 전용 액세스 권한.
Media Services 정책 관리자	웹	계정 필터, 스트리밍 정책, 콘텐츠 키 정책 및 변환을 생성, 읽기, 수정 및 삭제합니다.
Media Services 라이브 이벤트 관리자	웹	라이브 이벤트, 자산, 자산 필터 및 스트리밍 로케이터를 만들고, 읽고, 수정하고, 삭제합니다.
Media Services 스트리밍 엔드포인트 관리자	웹	스트리밍 엔드포인트 생성, 읽기, 수정 및 삭제, 다른 Media Services 리소스에 대한 읽기 전용 액세스 권한입니다.
Microsoft Sentinel 기여자	보안	Microsoft Sentinel 기여자
Microsoft Sentinel Automation 기여자	보안	Microsoft Sentinel Automation 기여자
Microsoft Sentinel 읽기 권한자	보안	Microsoft Sentinel 읽기 권한자
Site Recovery 운영자	관리+거버넌스	장애 조치(failover) 및 장애 복구(failback)를 수행할 수 있지만 다른 Site Recovery 관리 작업은 수행할 수 없습니다.

Site Recovery 참가자	관리+거버넌스	자격 증명 모음 만들기 및 역할 할당을 제외한 Site Recovery 서비스를 관리할 수 있습니다.
Site Recovery 열람자	관리+거버넌스	Site Recovery 상태를 볼 수 있지만 다른 관리 작업은 수행할 수 없습니다.
검색 인덱스 데이터 기여자	웹	Azure Cognitive Search 인덱스 데이터에 대한 전체 액세스 권한을 부여합니다.
검색 인덱스 데이터 읽기 권한자	웹	Azure Cognitive Search 인덱스 데이터에 대한 읽기 권한을 부여합니다.
계층 설정 관리자	관리+거버넌스	사용자가 계층 설정을 편집 및 삭제할 수 있습니다.
관리 ID 기여자	ID	사용자 할당 ID 의 만들기, 읽기, 업데이트 및 삭제
관리 ID 운영자	ID	사용자 할당 ID 의 읽기 및 할당
관리 그룹 독자	관리+거버넌스	관리 그룹 독자 역할
관리 그룹 참가자	관리+거버넌스	관리 그룹 참가자 역할
관리되는 HSM 기여자	보안	관리되는 HSM 풀을 관리할 수 있지만 액세스할 수는 없습니다.
관리형 애플리케이션 기여자 역할	관리+거버넌스	관리형 애플리케이션 리소스를 만들 수 있습니다.
관리되는 애플리케이션 운영자 역할	관리+거버넌스	관리되는 애플리케이션 리소스에서 작업을 읽고 수행할 수 있습니다.
관리되는 애플리케이션 판독기	관리+거버넌스	관리되는 앱에서 리소스를 읽고 JIT 액세스 권한을 요청할 수 있습니다.
데이터 제거자	분석	분석 데이터를 제거할 수 있음
디스크 백업 읽기 권한자	기타	디스크 백업을 수행하려면 백업 자격 증명 모음에 대한 권한을 제공합니다.
디스크 복원 운영자	기타	디스크 복원을 수행하려면 백업 자격 증명 모음에 대한 권한을 제공합니다.
디스크 스냅샷 기여자	기타	디스크 스냅샷을 관리하려면 백업 자격 증명 모음에 대한 권한을 제공합니다.
리소스 정책 참가자	관리+거버넌스	리소스 정책을 생성/수정하고, 지원 티켓을 만들고, 리소스/계층 구조를 읽을 수 있는 권한을 가진 사용자입니다.
모니터링 리더	모니터	모든 모니터링 데이터를 읽을 수 있습니다.
모니터링 메트릭 게시자	모니터	Azure 리소스에 대해 메트릭을 게시할 수 있습니다.
모니터링 참가자	모니터	모든 모니터링 데이터를 읽고 모니터링 설정을 업데이트할 수 있습니다.

보안 관리자	보안	보안 관리자 역할
보안 관리자(레거시)	보안	보안 관리자 레거시 역할
보안 평가 기여자	보안	Security Center 로 평가를 푸시할 수 있습니다.
보안 읽기 권한자	보안	보안 읽기 권한자 역할
사용자 액세스 관리자	일반	Azure 리소스에 대한 사용자 액세스를 관리할 수 있음
서비스 허브 운영자	기타	서비스 허브 운영자는 서비스 허브 커넥터와 관련된 모든 읽기, 쓰기 및 삭제 작업을 수행할 수 있습니다.
청구 리더	관리+거버넌스	결제 데이터에 대해 읽기 액세스 권한 허용
통합 문서 기여자	모니터링	공유 통합 문서를 저장할 수 있습니다.
통합 문서 읽기 권한자	모니터링	통합 문서를 읽을 수 있습니다.
할당량 요청 연산자	관리+거버넌스	할당량 요청을 읽고 만들고, 할당량 요청 상태를 가져오고, 지원 티켓을 만듭니다.

설정 방법

가. 기타 서비스 액세스 제어(IAM) 추가

1) 기타 서비스(키 자격 증명 모음) 목록 확인

2) 키 자격 증명 모음 내 IAM 역할 할당 추가

3) 서비스 목적에 맞는 역할 할당 추가

4) 역할 할당 구성원 추가

5) 역할 할당 검토

	6) 역할 할당 추가 완료 및 확인 
진단 기준	**양호기준** : 기타 서비스에 대한 액세스 제어(IAM)가 사용자 역할에 맞게 부여되어 있는 경우 **취약기준** : 기타 서비스에 대한 액세스 제어(IAM)가 사용자 역할에 맞게 부여되어 있지 않은 경우
비고	

3. 가상 리소스 관리

3.1 가상 네트워크 리소스 관리

<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">가상 네트워크 리소스 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure 가상 네트워크(Virtual Network)를 사용하면 Azure VM(Virtual Machines)과 같은 다양한 형식의 Azure 리소스가 서로 또는 인터넷 및 특정 온-프레미스 네트워크와 안전하게 통신할 수 있습니다. '연결된 디바이스' 메뉴를 통해 가상 네트워크에 연결되는 Azure 리소스를 확인할 수 있고, 해당 가상 네트워크에 불필요한 디바이스를 삭제할 수 있습니다.

※ 연결된 디바이스(VM)에 공용IP를 할당한 경우, IP 호출을 통해 직접 연결이 가능함.

※ 연결된 디바이스 관리 List (예시)
<table>
<tr><th>가상 네트워크</th><th>연결된 디바이스</th><th>서브넷</th><th>IP</th><th>사용목적</th><th>취약 유/무</th></tr>
<tr><td rowspan="3">RsGrpNet001</td><td>azurehvm400</td><td>ex)dafult_subnet</td><td>ex)10.0.0.1</td><td>ex)사용목적</td><td>N/A</td></tr>
<tr><td></td><td></td><td></td><td></td><td>N/A</td></tr>
<tr><td></td><td></td><td></td><td></td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 연결된 디바이스 목록 및 상세 확인
1) 가상 네트워크 메뉴 내 디바이스 목록을 확인할 가상 네트워크 선택
 

2) 연결된 디바이스 목록 메뉴 내 불필요하거나 알 수 없는 디바이스 존재 유무 확인
 

3) 공용 IP 주소 확인</td></tr>
</table>

나. 연결된 디바이스 제거 방법

1) 가상 네트워크 메뉴 내 디바이스 목록을 확인할 가상 네트워크 선택

2) 연결된 디바이스 목록 메뉴 내 불필요하거나 알 수 없는 디바이스 존재 유무 확인

3) 불필요하게 연결된 디바이스 삭제

다. 연결된 디바이스 내 공용 IP 주소 분리 방법

1) 가상 네트워크 메뉴 내 디바이스 목록을 확인할 가상 네트워크 선택

2) 연결된 디바이스 확인

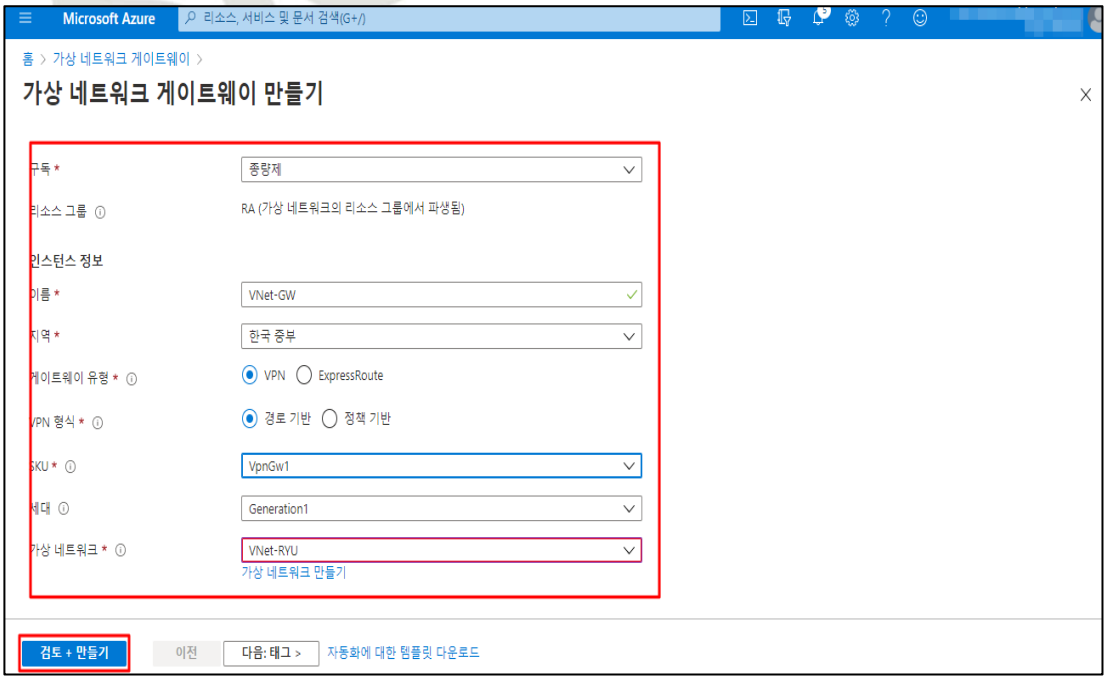
3) 공용 IP 주소 확인

4) 공용 IP 주소 내역 확인

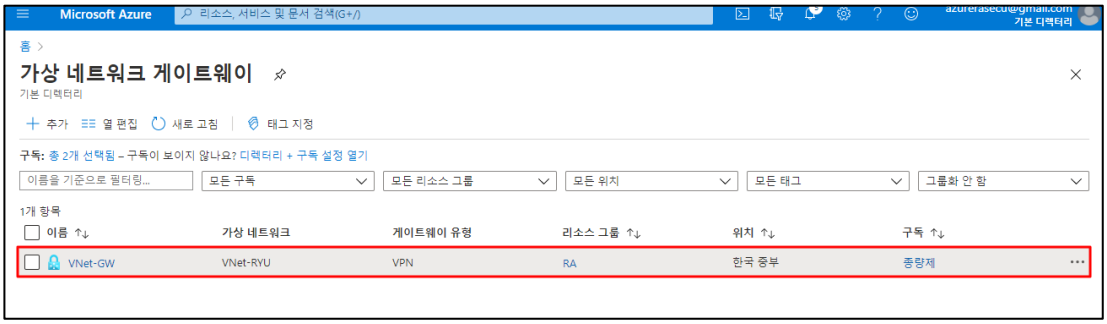
5) 공용 IP 주소 분리

	
진단 기준	**양호기준** : 연결된 디바이스 중 내부 네트워크만 사용하는 리소스에 공용 IP 주소가 존재하지 않는 경우 **취약기준** : 연결된 디바이스 중 내부 네트워크만 사용하는 리소스에 공용 IP 주소가 존재하는 경우
비고	

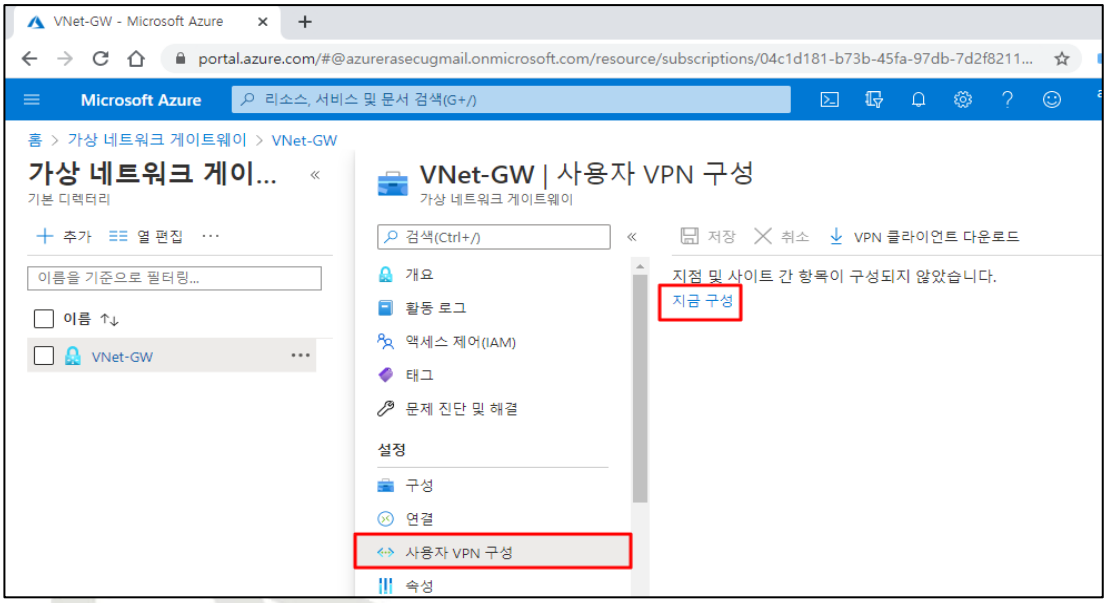
3.2 내부 가상 네트워크 보안 관리

분류	가상 리소스 관리	중요도	상
항목명	내부 가상 네트워크 보안 관리		
항목 설명	AZURE Virtual Private Network(AZURE VPN)를 이용하여 사용자 네트워크 또는 디바이스에서 AZURE 클라우드로 이어지는 안전한 프라이빗 터널을 설정할 수 있습니다. 기존의 온프레미스 네트워크를 VPC로 확장하거나 클라이언트에서 다른 AZURE 리소스에 연결할 수 있으며 AZURE VPN은 사용자 데이터를 위한 고 가용성과 강력한 보안이 보장되는 두 종류의 프라이빗 연결 기능을 제공합니다. 프라이빗 가상머신 접근 시 퍼블릭 가상머신을 통한 "Server to Server" 접근이 가능하다면, 외부 공격자에 의해 프라이빗 인스턴스로 접근하는 통로로 활용될 수 있으므로 AZURE에서 제공하는 VPN 또는 타사 VPN 소프트웨어를 통한 안전한 연결(IPsec 등)이 필요합니다.		
설정 방법	**가. 가상 네트워크 게이트웨이 사용자 VPN 연결 방법** 1) 가상 네트워크 게이트웨이 추가  2) 가상 네트워크 게이트웨이 정보 입력 및 만들기 		

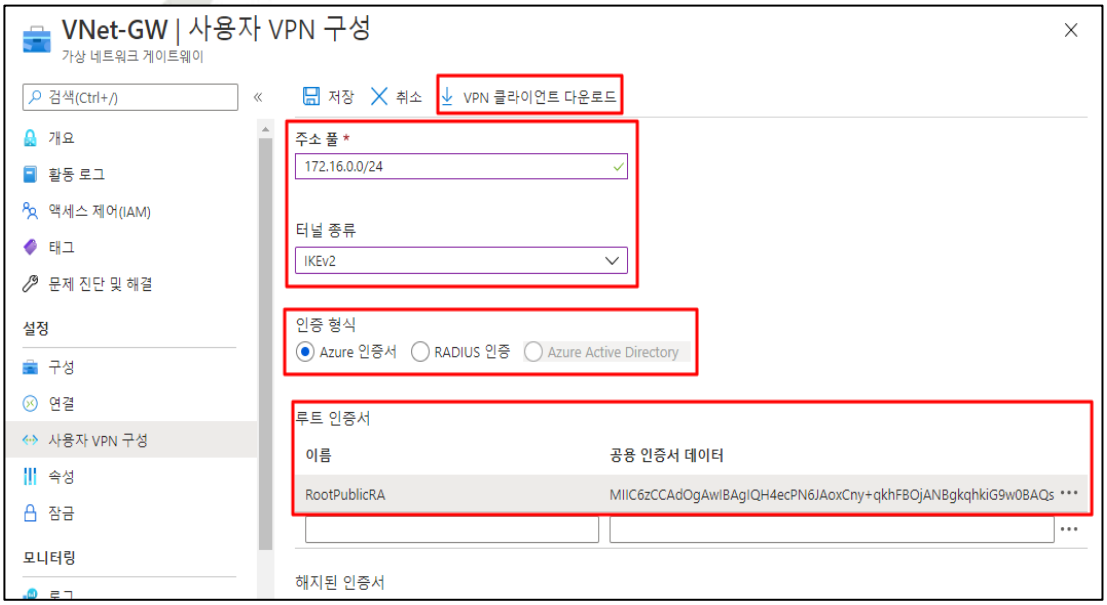
3) 생성된 가상 네트워크 게이트웨이 확인



4) 사용자 VPN 구성

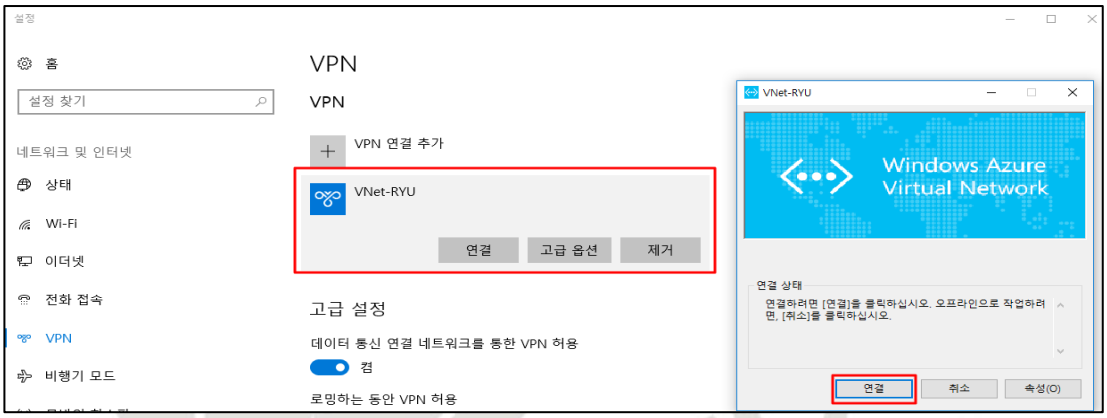


5) VPN 정보 입력, 인증서 등록 및 VPN 클라이언트 다운로드

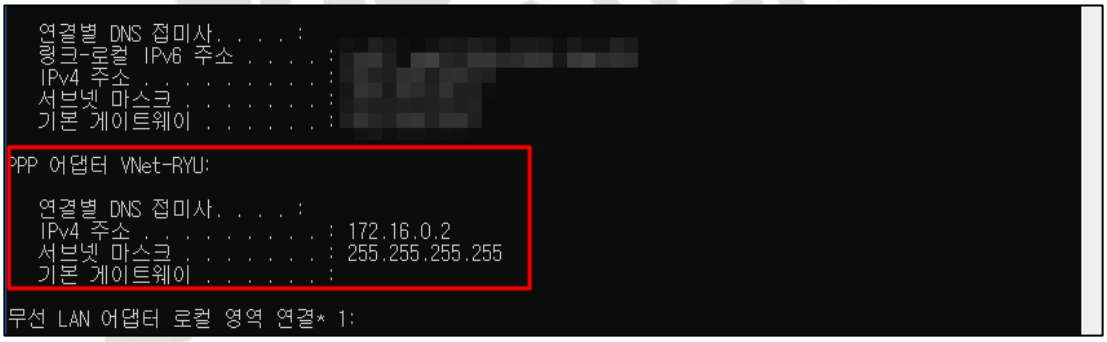


6) VPN 클라이언트 설치

7) 로컬에서 설치된 VPN 연결 시도

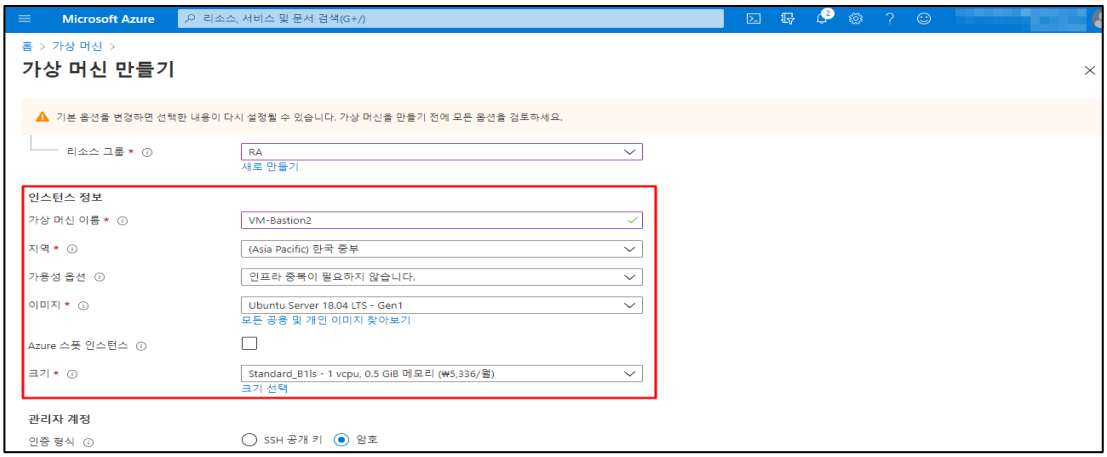


8) VPN 구성 시 설정한 주소 풀 IP 정보 확인

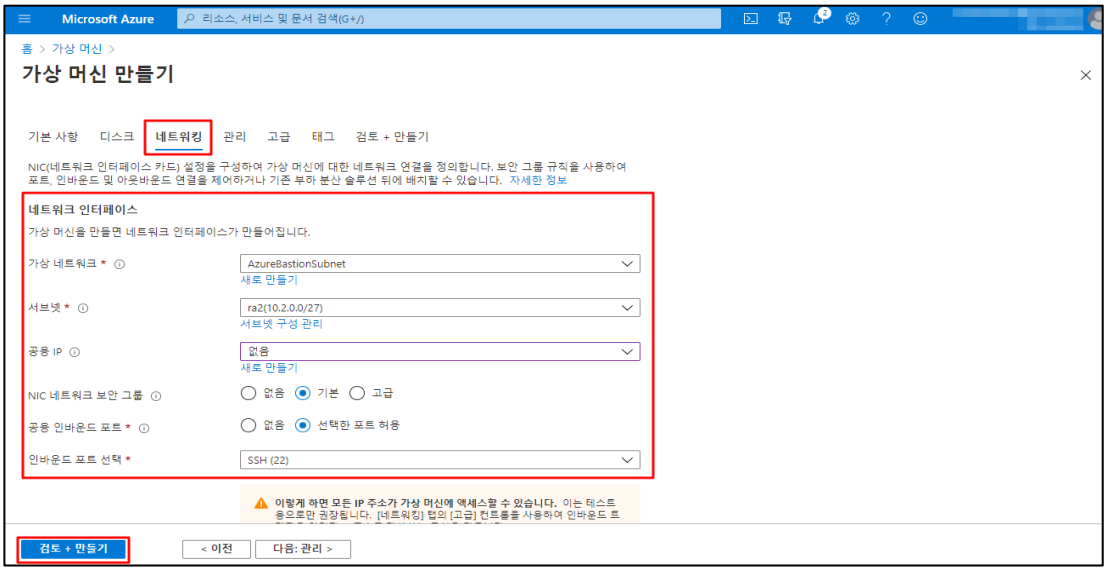


나. Bastion 가상 머신 이용한 연결

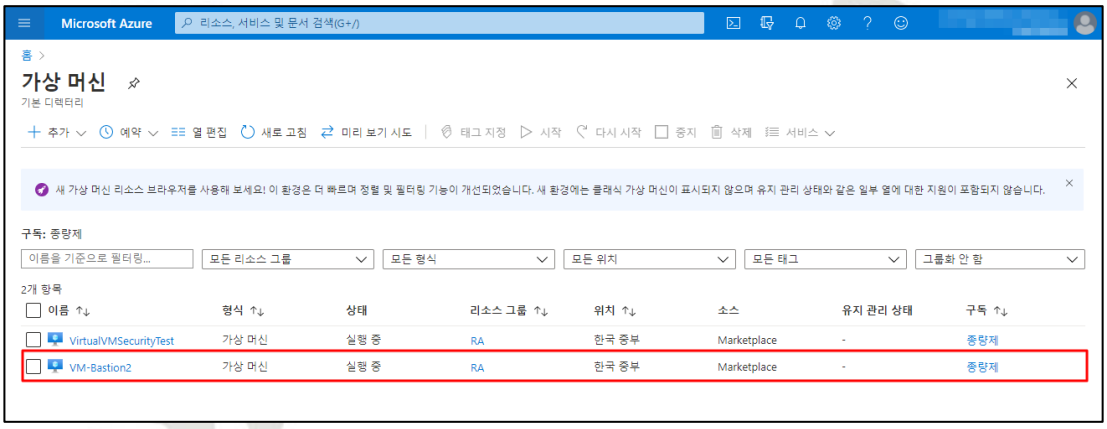
1) Bastion에 포함될 가상 머신 추가



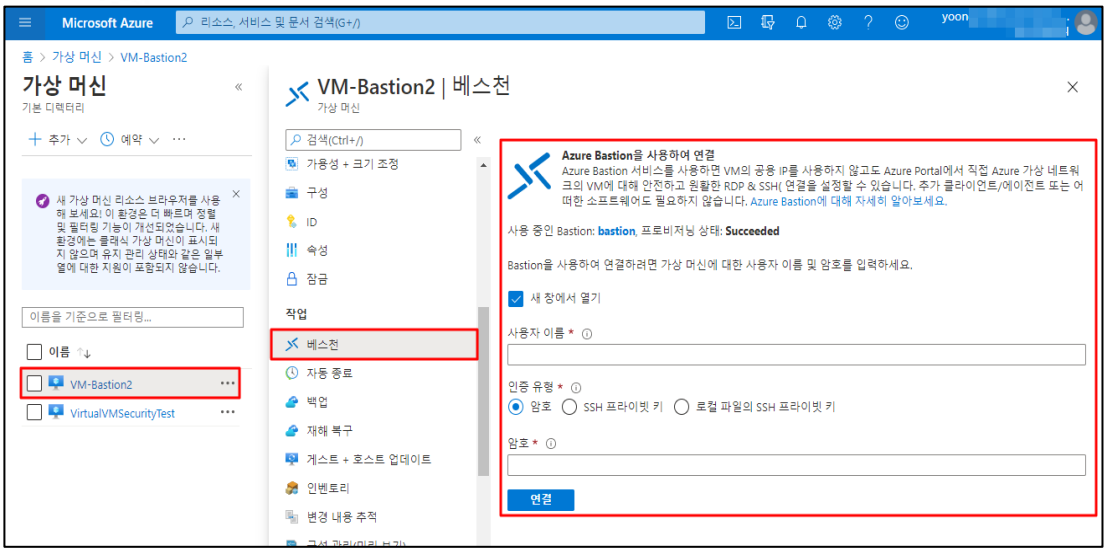
2) Bastion에 포함될 가상 네트워크 등록



3) 생성된 가상 머신 확인

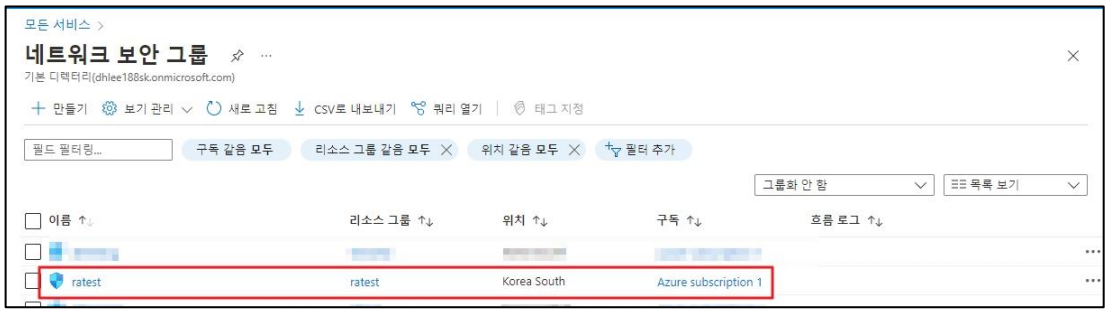


4) 가상 머신 내 Bastion 메뉴를 통해 연결 확인



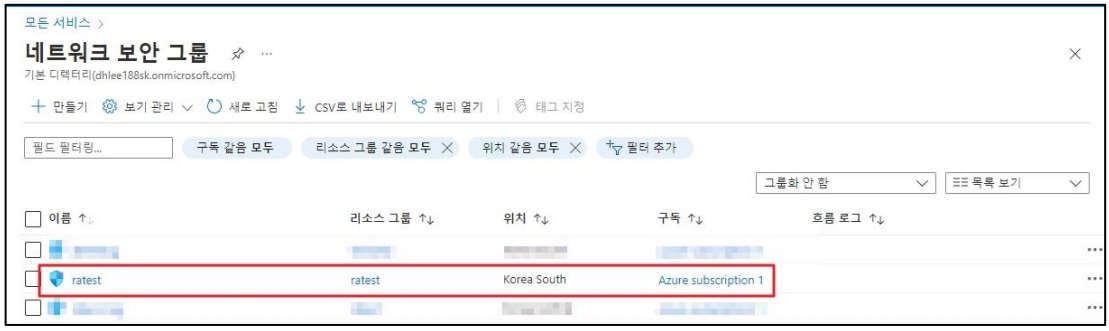
진단 기준	**양호기준** : 내부 리소스 접근 시 접근통제(VPN, Bastion)가 적용되어 있을 경우 **취약기준** : 내부 리소스 접근 시 접근통제(VPN, Bastion)가 적용되어 있지 않을 경우
비고	

3.3 보안그룹 인/아웃바운드 ANY 설정 관리

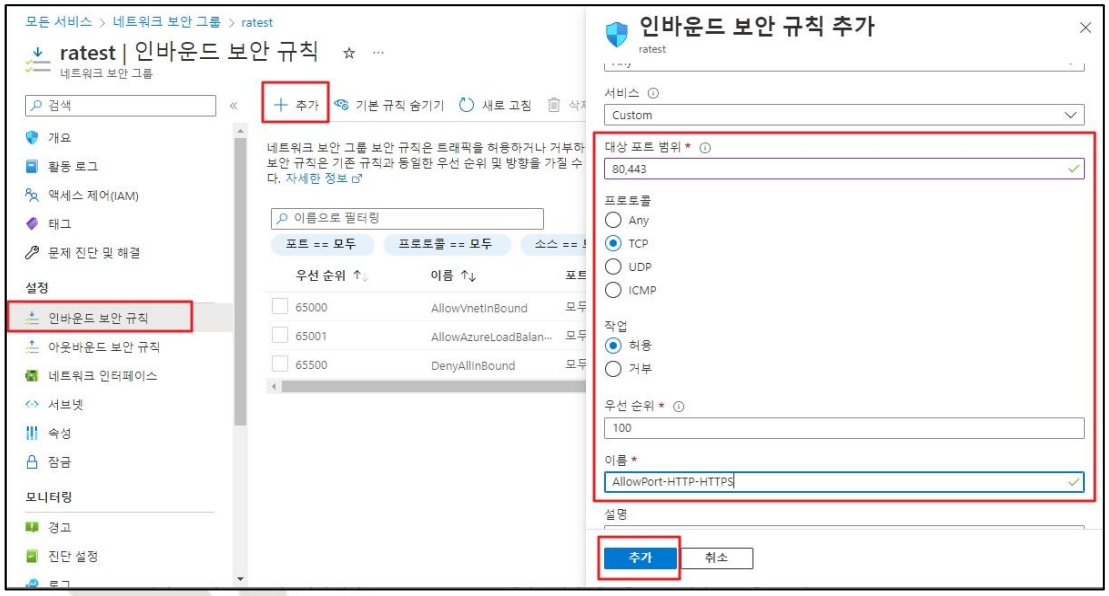
분류	가상 리소스 관리	중요도	상
항목명	보안그룹 인/아웃바운드 ANY 설정 관리		
항목 설명	네트워크 보안 그룹 (Security Group)은 가상머신에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할로서 네트워크 리소스에서 가상머신을 시작할 때 서브넷 수준이 아니라 가상머신 수준에서 작동하므로 네트워크 리소스에 있는 서브넷의 각 가상머신을 서로 다른 보안 그룹 세트에 할당할 수 있습니다. 보안그룹은 네트워크 리소스 별 규칙을 추가하거나 제거가 가능하며 인바운드 트래픽(수신)이나 아웃바운드 트래픽(송신)에 적용되므로 불필요하게 Any로 허용된 Port가 존재할 경우 AZURE 리소스에 비정상적인 접근 또는 2차 공격에 활용될 수 있습니다.		
설정 방법	**가. 네트워크 보안 그룹 생성** 1) 네트워크 보안 그룹 만들기  2) 네트워크 보안 그룹 정보 입력 및 만들기  3) 네트워크 보안 그룹 생성 완료 및 확인  		

나. 네트워크 보안 그룹 Port 설정

1) 네트워크 보안 그룹 선택



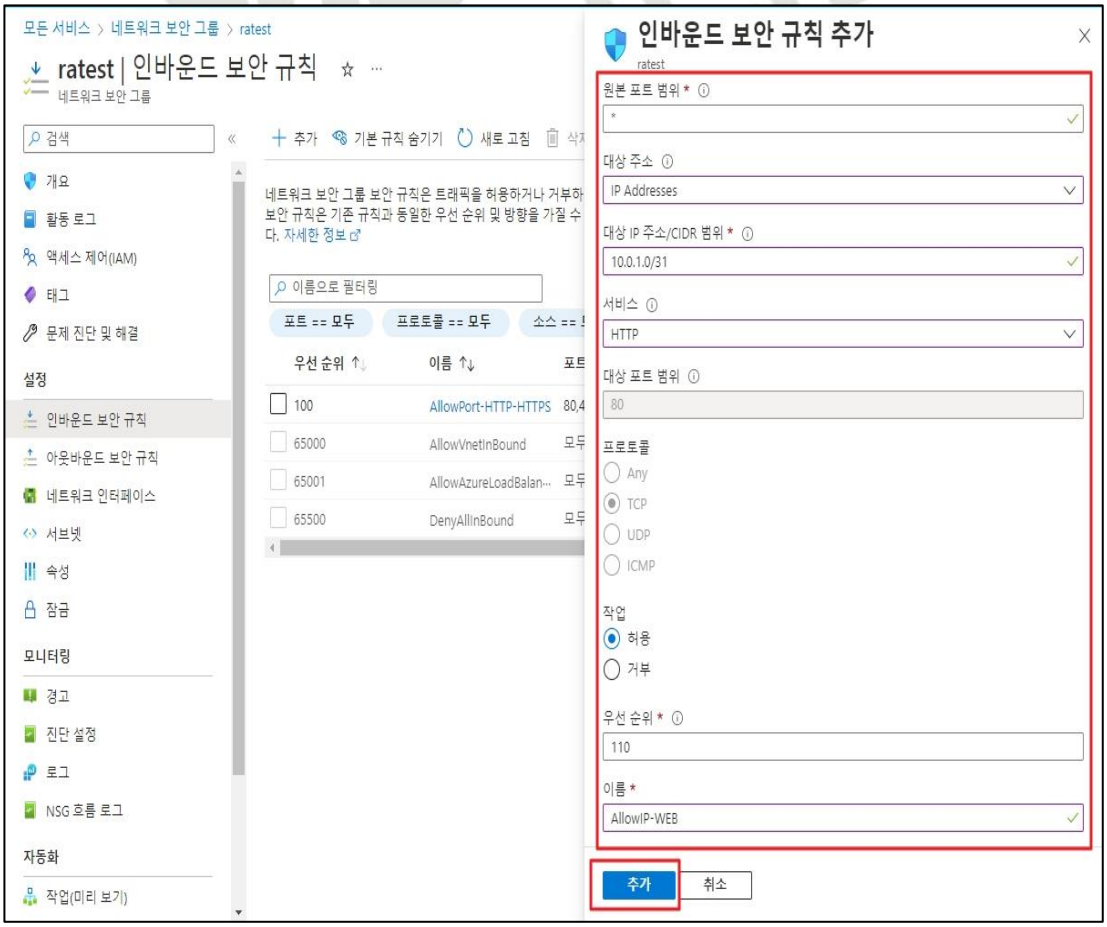
2) 서비스에 필요한 인바운드 보안 규칙(Port) 추가



3) 인바운드 보안 규칙(Port) 생성 및 확인

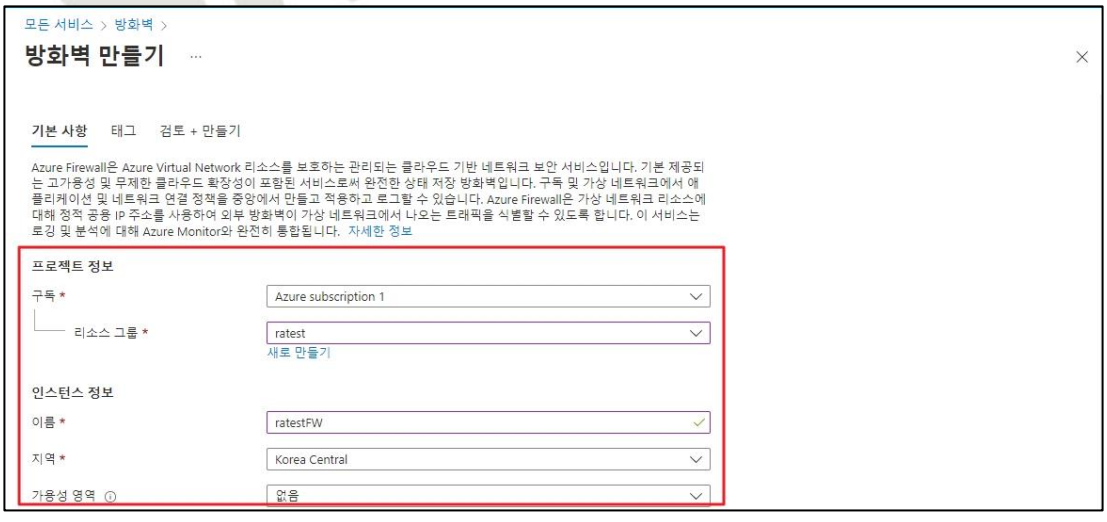
진단 기준	**양호기준** : 보안그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있지 않을 경우 **취약기준** : 보안그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있을 경우
비고	

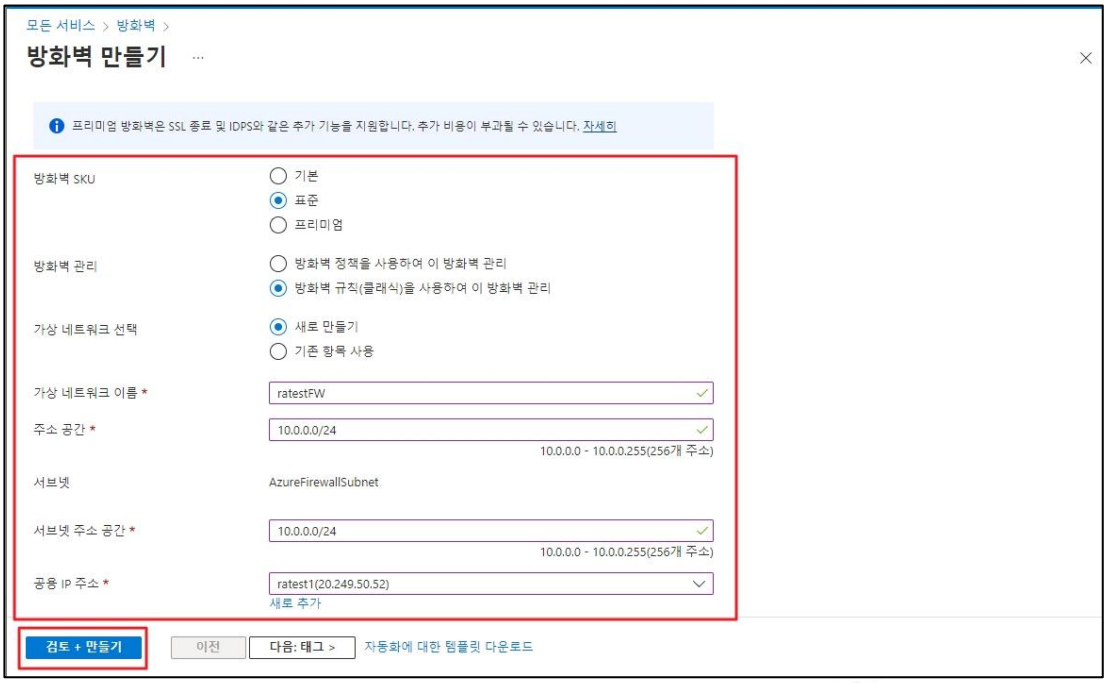
3.4 보안그룹 인/아웃바운드 불필요 정책 관리

분류	가상 리소스 관리	중요도	중
항목명	보안그룹 인/아웃바운드 불필요 정책 관리		
항목 설명	네트워크 보안 그룹 (Security Group)은 네트워크 규칙(Source, Destination)을 추가하거나 제거가 가능하며 인바운드 트래픽(수신)이나 아웃바운드 트래픽(송신)에 적용되므로 불필요한 정책이 존재할 경우 AZURE 리소스에 비정상적인 접근 또는 2차 공격에 활용될 수 있습니다.		
설정 방법	**가. 네트워크 보안 그룹 IP Address 설정** 1) 네트워크 보안 그룹 선택  2) 서비스에 필요한 인바운드 보안 규칙(IP Address) 추가 		

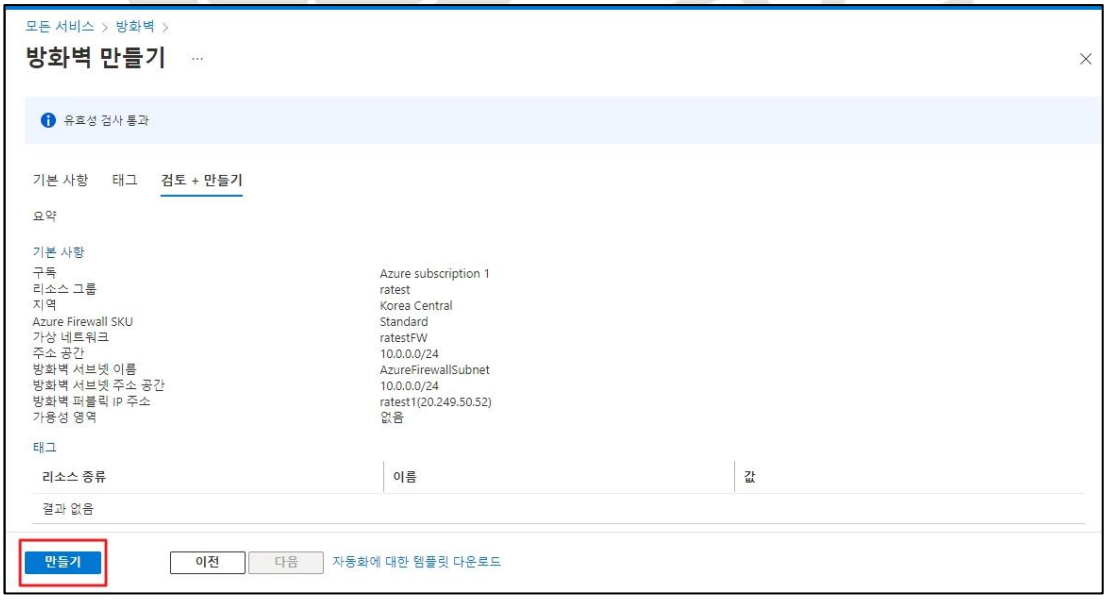
	3) 인바운드 보안 규칙(IP Address) 생성 및 확인 
진단 기준	**양호기준** : 보안그룹 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하지 않는 경우 **취약기준** : 보안그룹 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하는 경우
비고	

3.5 방화벽 ANY 정책 설정 관리

분류	가상 리소스 관리	중요도	상
항목명	방화벽 ANY 정책 설정 관리		
항목 설명	Azure Firewall은 Azure Virtual Network 리소스를 보호하는 관리되는 클라우드 기반 네트워크 보안 서비스입니다. 고 가용성 및 무제한 클라우드 확장성이 내장되어 있는 서비스 형태의 완전한 상태 저장 방화벽입니다. 방화벽 정책 내 ANY 규칙이 존재할 경우 Azure 리소스에 비정상적인 접근 또는 2차 공격에 활용될 수 있으므로, 설정되어 있는 정책의 출발지와 목적지의 IP주소 범위, 프로토콜/Port, 허용/차단, 정책 순서 등을 종합적으로 검증하여 방화벽 ANY 규칙이 존재하지 않는지 주기적으로 확인해야 합니다. **※ 해당 기능은 필수적으로 설치되는 기능이 아닌 추가 비용이 부과되는 기능입니다. (고비용)**		
설정 방법	**가. 방화벽 생성 방법** 1) 방화벽 메뉴 내 만들기 버튼 선택  2) 방화벽 설정 값 입력  		



3) 방화벽 설정 값 검토 및 만들기



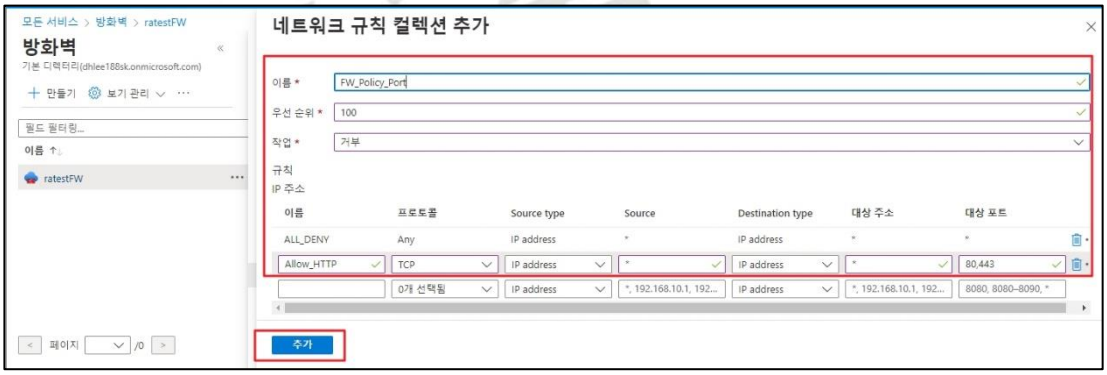
4) 방화벽 정상 생성 유무 확인

나. 방화벽 네트워크 규칙 생성 방법

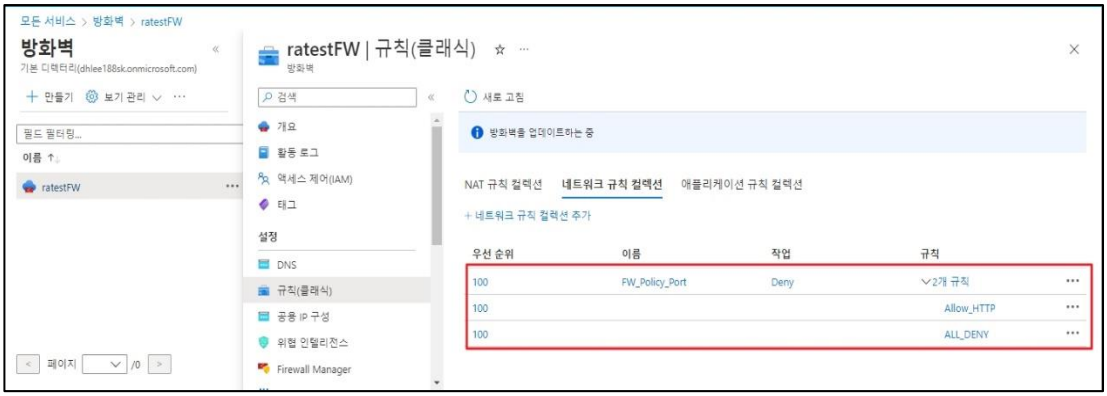
1) 방화벽 메뉴 내 네트워크 규칙을 추가할 방화벽 선택

2) 규칙 메뉴 내 네트워크 규칙 컬렉션 추가 버튼 선택

3) 추가할 규칙 설정 및 추가



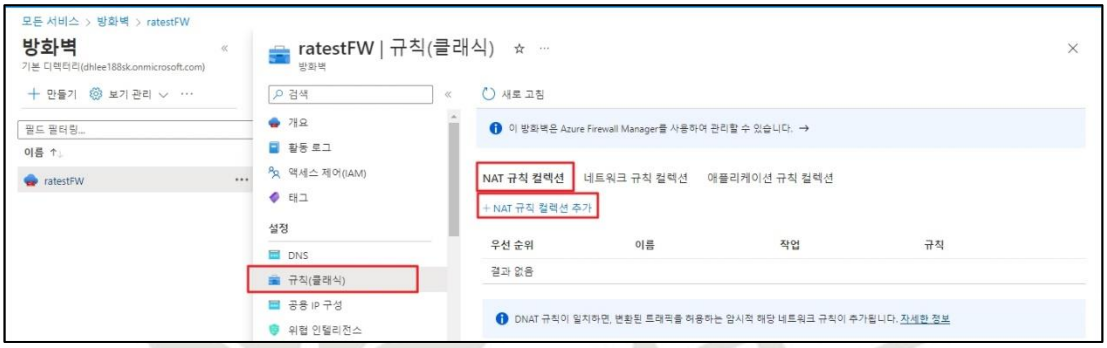
4) 네트워크 규칙 정상 생성 유무 확인



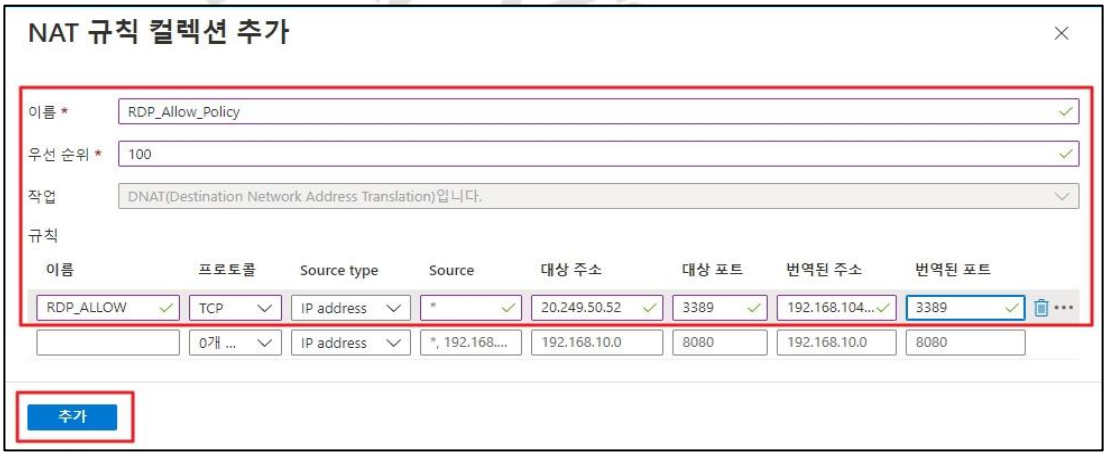
다. 방화벽 NAT 규칙 생성 방법

1) 방화벽 메뉴 내 NAT 규칙을 추가할 방화벽 선택

2) 규칙 메뉴 내 NAT 규칙 컬렉션 추가 버튼 선택



3) 추가할 규칙 설정 및 추가



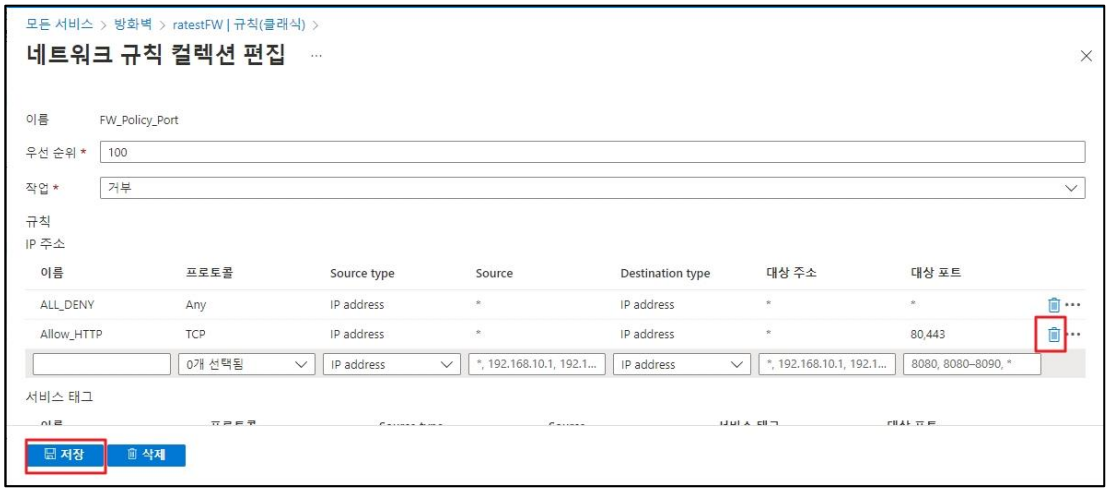
4) NAT 규칙 정상 생성 유무 확인

진단 기준	**양호기준** : 방화벽 정책 내 규칙(Source, Destination, Port)이 Any로 허용되어 있지 않을 경우 **취약기준** : 방화벽 정책 내 규칙(Source, Destination, Port)이 Any로 허용되어 있을 경우
비고	

3.6 방화벽 불필요 정책 관리

분류	가상 리소스 관리	중요도	중
항목명	방화벽 불필요 정책 관리		
항목 설명	Azure Firewall은 Azure Virtual Network 리소스를 보호하는 관리되는 클라우드 기반 네트워크 보안 서비스입니다. 고 가용성 및 무제한 클라우드 확장성이 내장되어 있는 서비스 형태의 완전한 상태 저장 방화벽입니다. 방화벽 정책 내 불필요한 규칙이 존재할 경우 Azure 리소스에 비정상적인 접근 또는 2차 공격에 활용될 수 있으므로, 설정되어 있는 정책의 출발지와 목적지의 IP주소 범위, 프로토콜/Port, 허용/차단, 정책 순서 등을 종합적으로 검증하여 불필요한 방화벽 규칙이 존재하지 않는지 주기적으로 확인해야 합니다. **※ 해당 기능은 필수적으로 설치되는 기능이 아닌 추가 비용이 부과되는 기능입니다. (고비용)**		
설정 방법	**가. 방화벽 내 불필요한 네트워크 규칙 삭제 방법** 1) 방화벽 메뉴 내 네트워크 규칙을 삭제할 방화벽 선택  2) 규칙 메뉴 내 네트워크 규칙을 삭제할 규칙 컬렉션 선택 		

3) 개별 규칙 삭제 버튼 선택



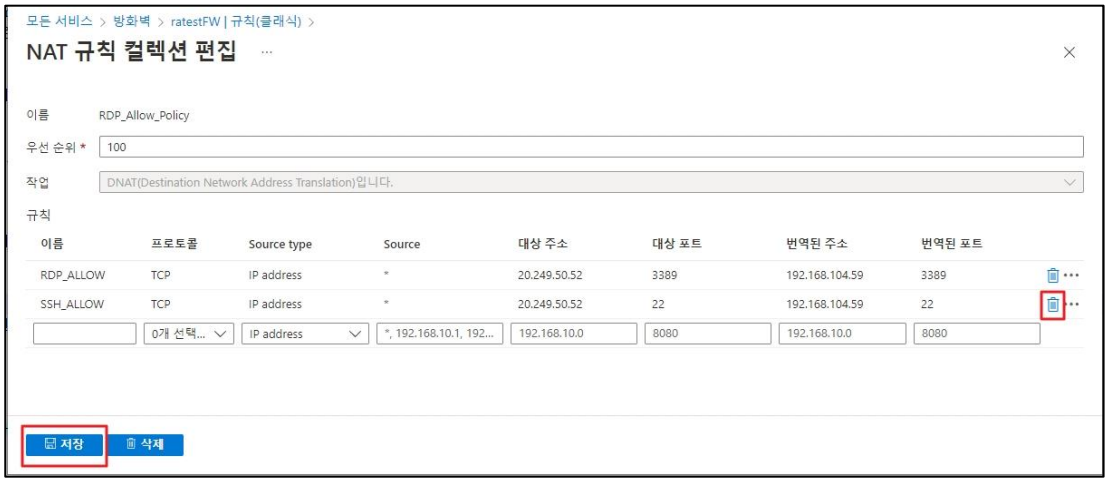
4) 네트워크 규칙 정상 삭제 유무 확인

나. 방화벽 내 불필요한 NAT 규칙 삭제 방법

1) 방화벽 메뉴 내 NAT 규칙을 삭제할 방화벽 선택

2) 규칙 메뉴 내 NAT 규칙을 삭제할 규칙 컬렉션 선택

3) 개별 규칙 삭제 버튼 선택



4) NAT 규칙 정상 삭제 유무 확인

진단 기준

양호기준

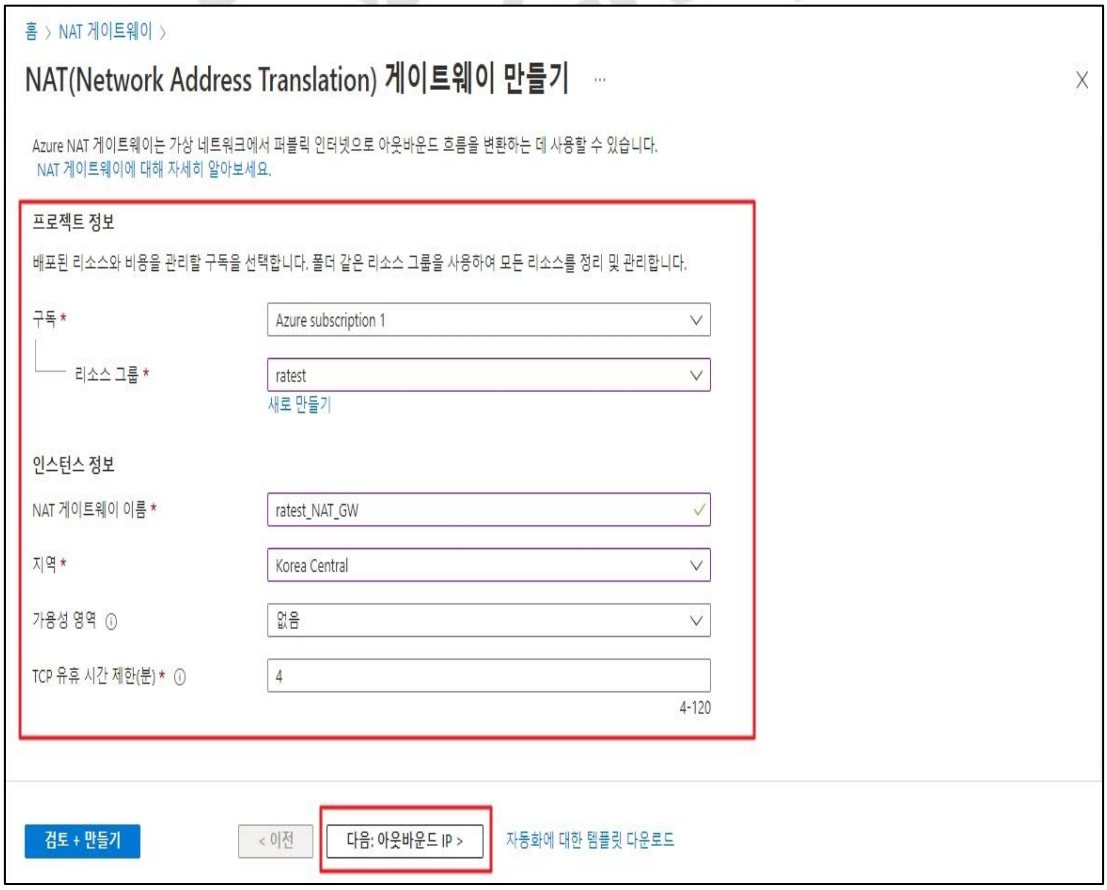
: 방화벽 정책 내 불필요한 규칙이 존재하고 있지 않을 경우

취약기준

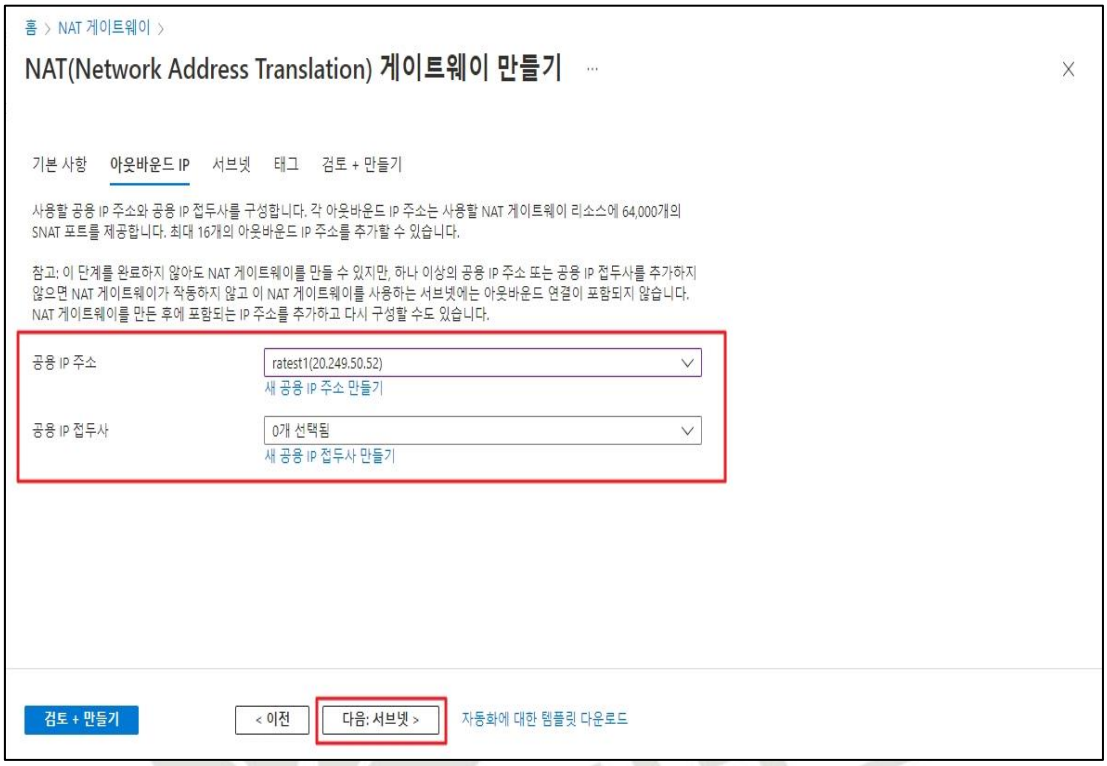
: 방화벽 정책 내 불필요한 규칙이 존재하고 있을 경우

비고

3.7 NAT 게이트웨이 서브넷 연결 관리

분류	가상 리소스 관리	중요도	중
항목명	NAT 게이트웨이 서브넷 연결 관리		
항목 설명	NAT 게이트웨이는 하나 이상의 서브넷과 연결될 수 있는 복원력이 뛰어난 완전 관리형 서비스로, 모든 아웃바운드 인터넷 연결 트래픽이 게이트웨이를 통해 라우팅되도록 합니다. NAT 게이트웨이는 가상 네트워크의 하나 이상의 서브넷에 대한 아웃바운드 인터넷 연결을 제공합니다. NAT 게이트웨이가 서브넷에 연결되면 NAT는 해당 서브넷에 대한 SNAT(원본 네트워크 주소 변환)를 제공합니다.		
설정 방법	**가. NAT 게이트웨이 생성 및 서브넷 연결 확인** 1) NAT 게이트웨이 만들기 버튼 클릭  2) NAT 게이트웨이 기본 사항 입력 		

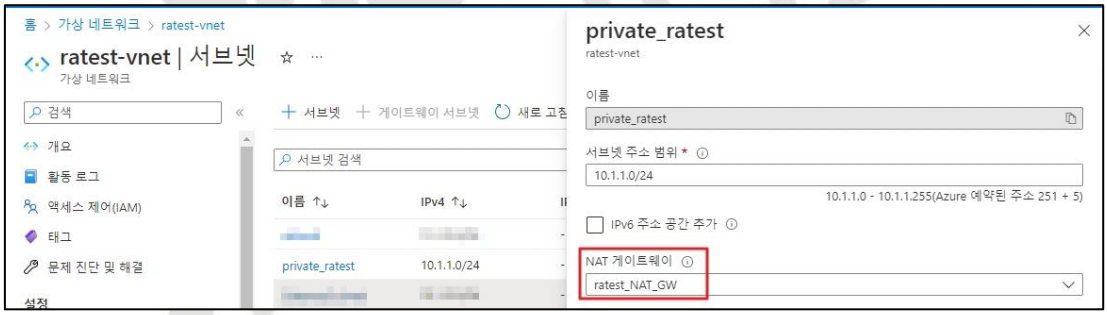
3) NAT 게이트웨이 아웃바운드 IP 입력



4) 퍼블릭 네트워크 접속이 필요한 서브넷 선택

5) NAT 게이트웨이 만들기 최종 검토 및 만들기

6) NAT 게이트웨이 생성 확인



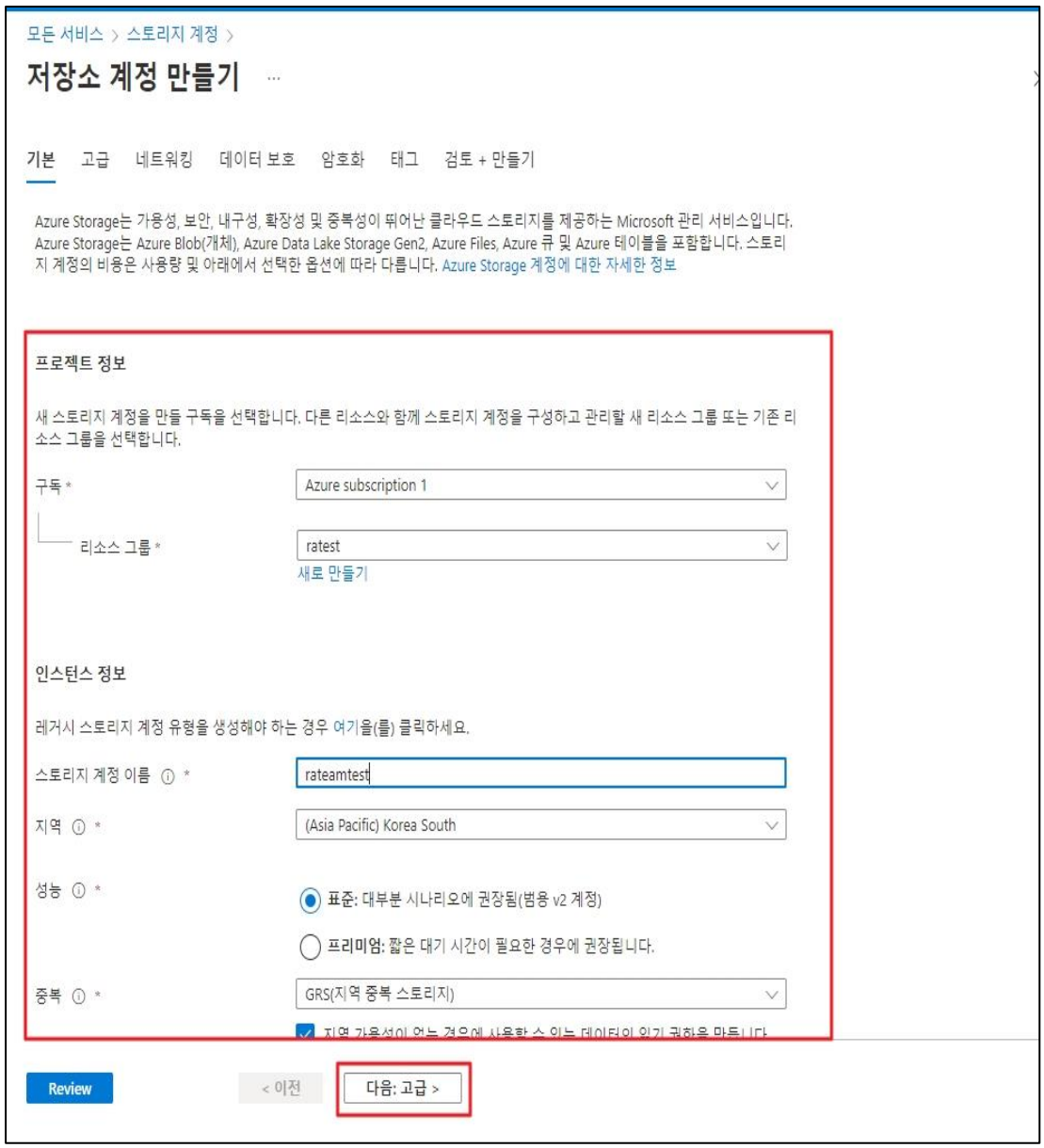
진단 기준	**양호기준** : 퍼블릭 네트워크 접속이 필요한 서브넷만 연결되어 있을 경우 **취약기준** : 퍼블릭 네트워크 접속이 불필요한 서브넷이 연결되어 있을 경우
비고	

3.8 스토리지 계정 보안 설정

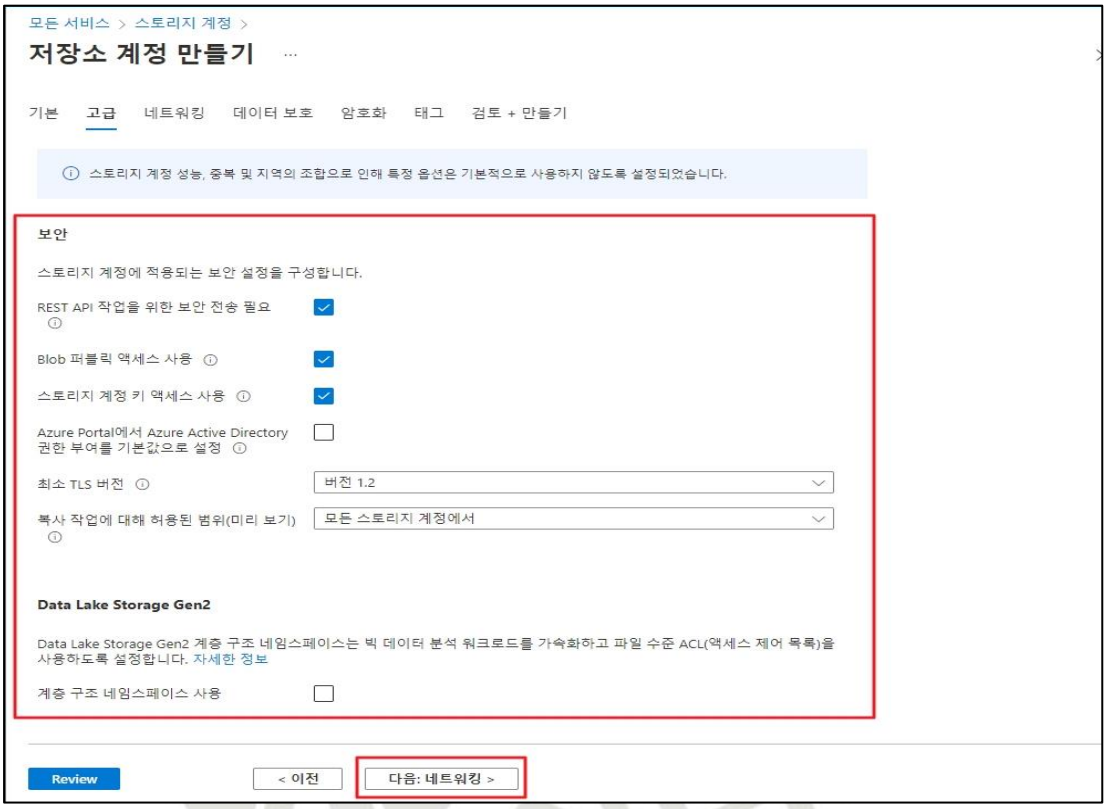
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">스토리지 계정 보안 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure 스토리지 계정에는 Blob, 파일, 큐, 테이블, 디스크 등 모든 Azure 스토리지 데이터 개체가 포함됩니다. 스토리지 계정은 Azure 스토리지 데이터에 대한 고유한 네임 스페이스를 제공하며 전 세계 어디에서나 HTTP 또는 HTTPS를 통해 접근할 수 있게 합니다. Azure 스토리지 계정의 데이터는 내구성 및 고 가용성을 제공하며 안전하고 대규모로 확장 가능합니다.

※ 스토리지 계정 생성 시 보안옵션
<table>
<tr><th>옵션</th><th>내용</th></tr>
<tr><td>REST API 작업을 위한 보안 전송 필요</td><td>보안 전송 옵션은 HTTP를 사용하는 스토리지 계정에 대한 REST API 작업만 허용함으로써 스토리지 계정의 보안을 강화합니다. 이 설정을 사용하면 HTTP를 사용하는 모든 요청이 거부됩니다</td></tr>
<tr><td>Blob 퍼블릭 액세스 사용</td><td>Blob 퍼블릭 액세스를 사용하도록 설정하면 사용자가 컨테이너 ACL을 구성하여 스토리지 계정 내 Blob에 익명 액세스를 허용할 수 있습니다. Blob 퍼블릭 액세스를 사용하지 않도록 설정하면 기본 ACL 구성과 관계없이 스토리지 계정 내 Blob에 익명 액세스가 허용되지 않습니다</td></tr>
<tr><td>스토리지 계정 키 액세스 사용</td><td>스토리지 계정 키 액세스를 사용하지 않도록 설정하면 SAS(공유 액세스 서명) 등 공유 키를 사용하여 권한이 부여된 계정에 대한 모든 요청이 거부됩니다.</td></tr>
<tr><td>Azure Portal에서 Azure Active Directory 권한 부여를 기본값으로 설정</td><td>이 속성을 사용하도록 설정하면 Azure Portal은 기본값으로 Azure Active Directory를 사용하여 Blob, 큐 및 테이블에 대한 요청에 권한을 부여합니다.</td></tr>
<tr><td>최소 TLS 버전</td><td>스토리지 계정의 데이터를 사용하여 애플리케이션에 필요한 최소 TLS 버전을 설정합니다.</td></tr>
<tr><td>복사 작업에 대해 허용된 범위</td><td>동일한 Azure AD 테넌트 내에 있거나 이 스토리지 계정과 동일한 가상 네트워크에 대한 프라이빗 링크가 있는 원본 스토리지 계정으로부터의 복사 작업을 제한합니다.</td></tr>
<tr><td>데이터 보호</td><td>Blob 일시삭제를 통해 응용 프로그램 또는 다른 스토리지 계정 사용자에 의해 잘못 수정되거나 삭제될 때 데이터를 보다 쉽게 복구</td></tr>
<tr><td>계층구조 네임스페이스</td><td>빅데이터 워크로드 분석을 가속화하고 파일단위 ACL을 활성화</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 스토리지 계정 생성 방법
1) 스토리지 계정 메뉴 내 만들기 버튼 선택</td></tr>
</table>

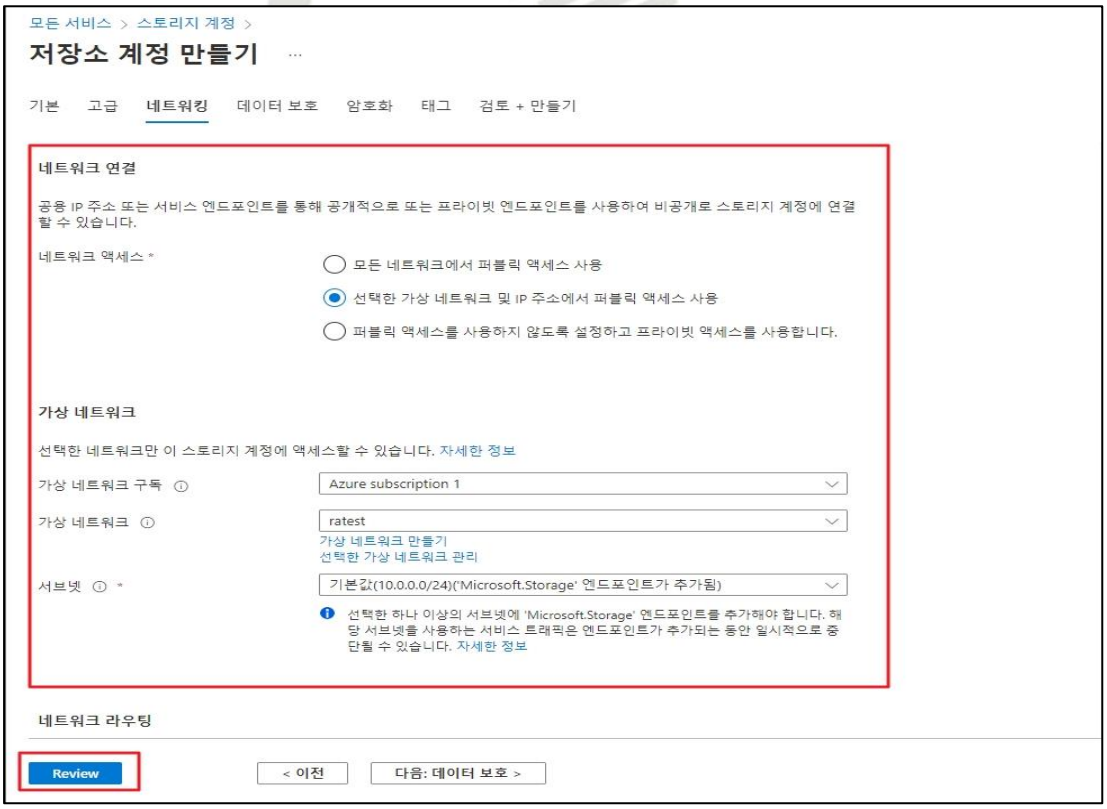
2) 스토리지 계정 관련 기본 사항 값 설정



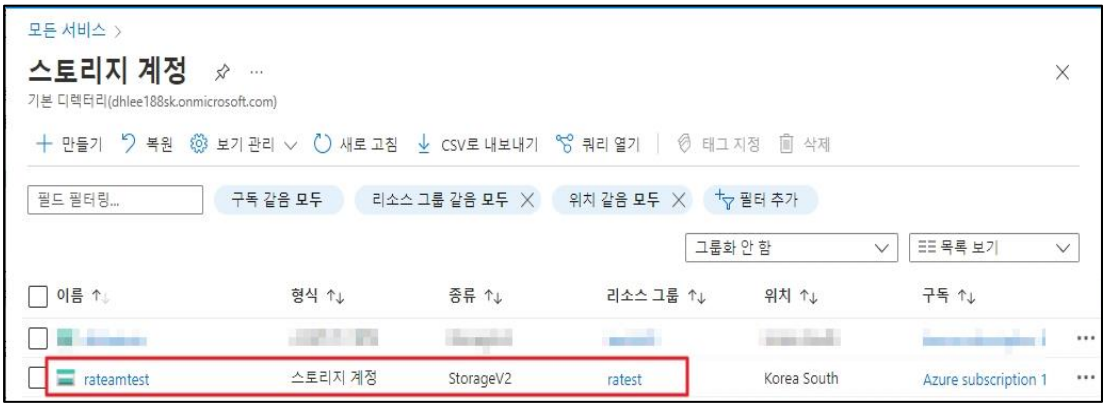
3) 스토리지 계정 관련 보안 옵션값 설정



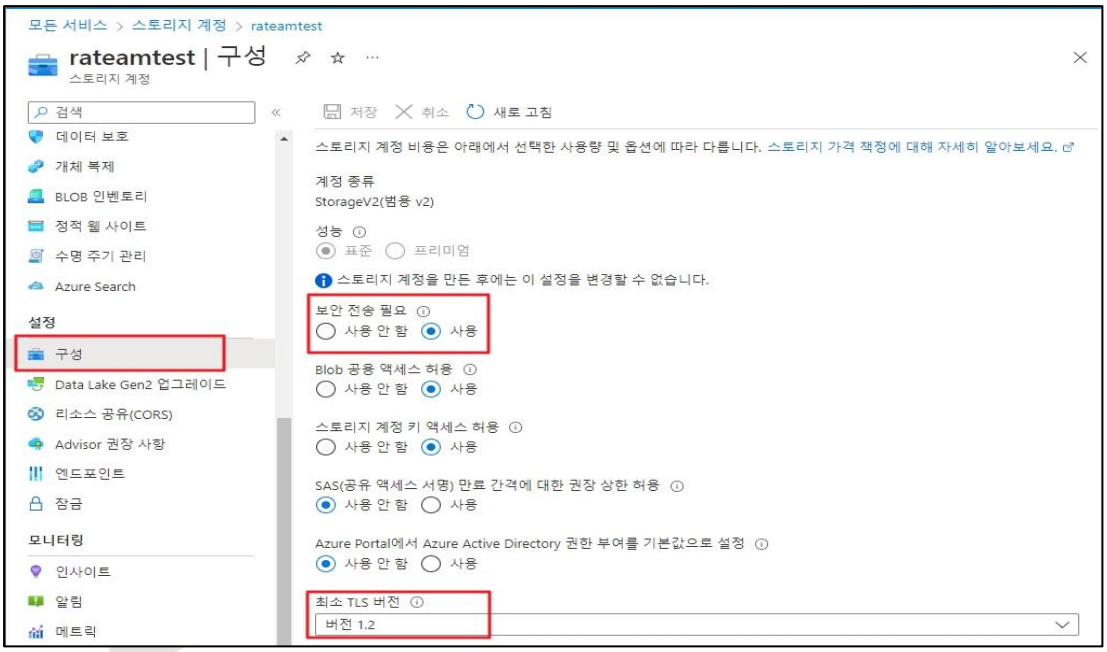
4) 스토리지 계정 관련 네트워킹 옵션값 설정



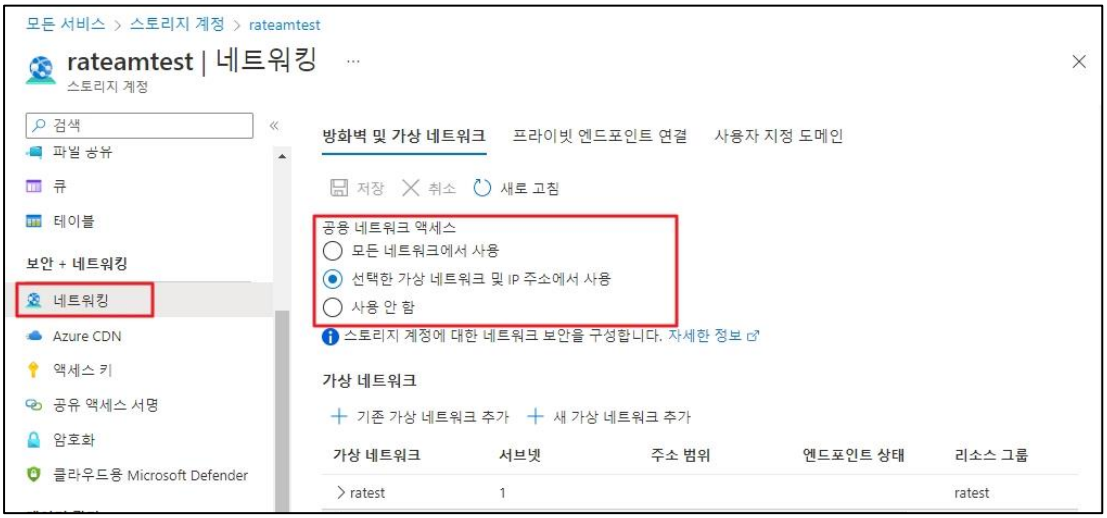
5) 스토리지 계정 목록 내 정상 생성 유무 확인



6) 스토리지 계정 메뉴 내 보안 옵션 확인



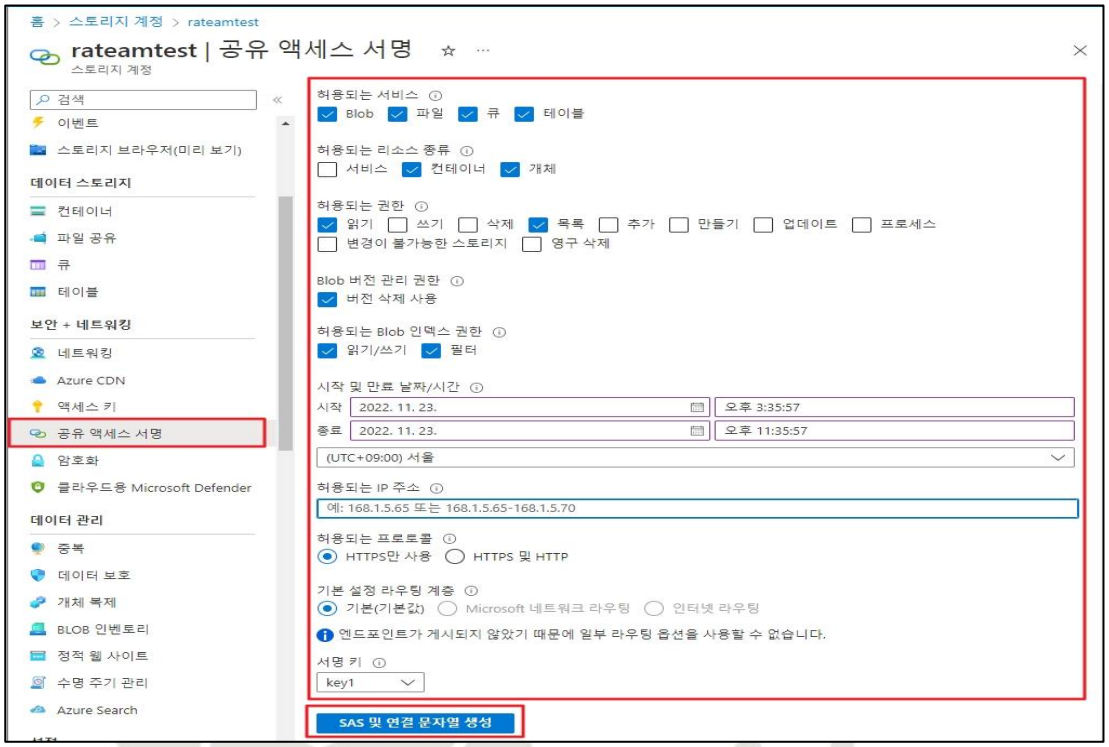
7) 공용 네트워크 액세스 설정



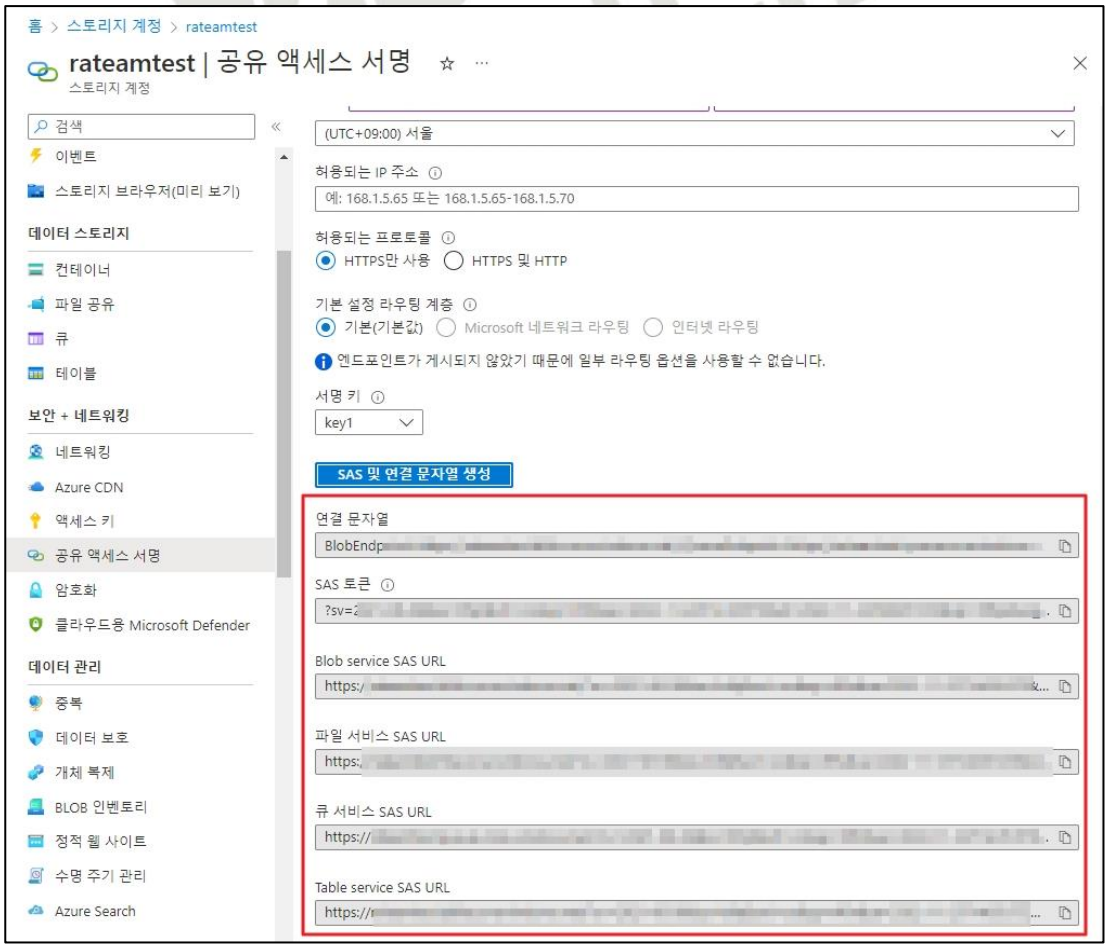
진단 기준	**양호기준** : 보안 전송 필요 활성화, TLS 버전(1.2) 설정 및 퍼블릭 액세스가 차단되어 있을 경우 **취약기준** : 보안 전송 필요 비활성화, TLS 버전(1.2 이하) 설정 및 퍼블릭 액세스가 차단되어 있을 경우
비고	

3.9 스토리지 계정 공유 액세스 서명 정책 관리

분류	가상 리소스 관리	중요도	중
항목명	스토리지 계정 공유 액세스 서명 정책 관리		
항목 설명	공유 액세스 서명은 하나 이상의 저장소 리소스를 가리키는 서명된 URI로, 특정 기간 동안 저장소 계정의 리소스에 대한 위임된 권한을 제공합니다. 키가 노출될 경우 악의적 또는 잘못된 사용이 가능해지기 때문에 리소스에 대한 액세스 권한 및 허용 IP가 최소한으로 부여되어 있어야 합니다. **※ 가상 스토리지 공유 액세스 서명(SAS) 설정 가능 항목** - 서비스 / 리소스 별 허용된 권한 - 시작시간 / 만료시간 - 허용 IP 또는 IP범위 - 허용 프로토콜		
설정 방법	**가. 가상 스토리지 공유 액세스 서명 (SAS) 생성 방법** 1) 스토리지 계정 메뉴 내 공유 액세스 서명을 생성할 스토리지 계정 선택  2) 공유 액세스 서명 메뉴 내 관련 값(서비스, 권한, 시작/만료날짜, IP, 통신프로토콜) 설정		



3) 각 서비스 별 공유 액세스 서명 URL 정상 생성 여부 확인



진단 기준	**양호기준** : 공유 액세스 서명을 사용 시 허용된 권한 및 허용 IP 주소가 최소한으로 설정되어 있을 경우 **취약기준** : 공유 액세스 서명을 사용 시 허용된 권한 및 허용 IP 주소가 최소한으로 설정되어 있지 않을 경우
비고	

4. 운영 관리

4.1 데이터베이스 암호화 설정 관리

<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">데이터베이스 암호화 설정 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">투명한 데이터 암호화 (TDE)는 SQL서버, 데이터베이스 등에서 미사용 데이터를 암호화 하여 오프라인 활동으로부터 데이터를 보호하는 기법입니다. TDE는 애플리케이션에 대한 변경없이 미사용 데이터베이스, 연결된 백업 및 트랜잭션 로그 파일의 실시간 암호화 및 암호해독을 수행합니다. 기본적으로 활성화 된 SQL 데이터베이스에는 TDE 설정이 활성화 되어 있으며, SQL서버의 경우 Key Vault를 사용한 사용자 고유키를 설정할 수 있으며 고유키의 만료일자 설정을 통해 제한적으로 사용으로 보안성을 보다 더 높일 수 있습니다.

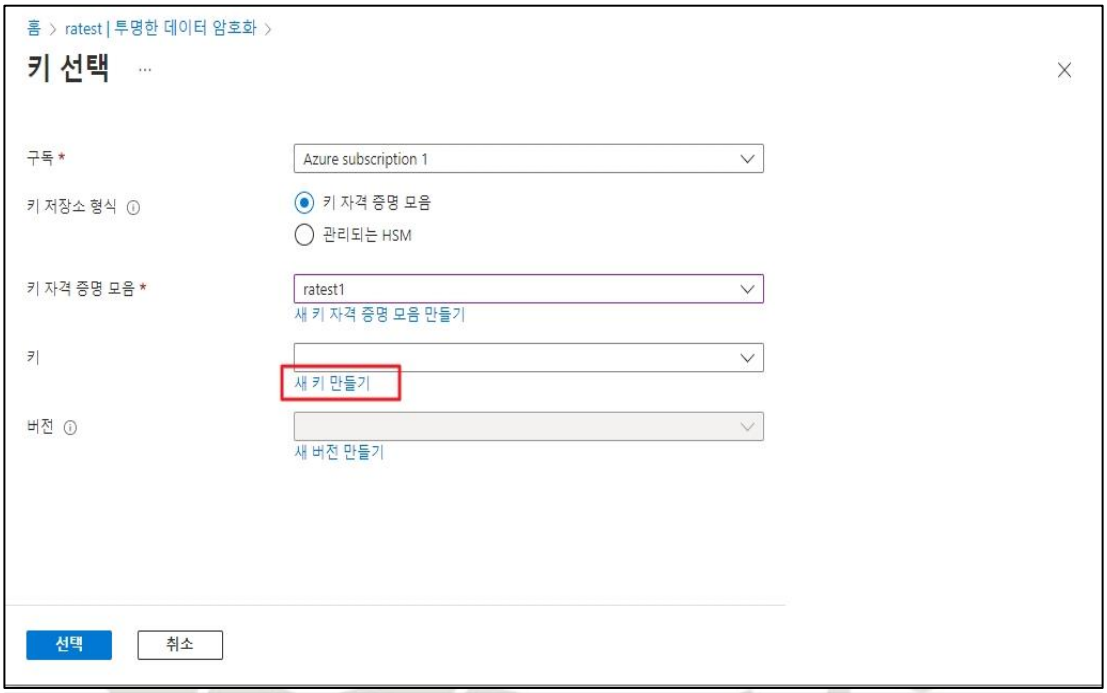
※ 데이터 암호화 대상 서비스
<table>
<tr><th>구분</th><th>서비스명</th><th>상세설명</th></tr>
<tr><td rowspan="3">투명한 데이터 암호화</td><td>SQL
데이터베이스</td><td>Azure SQL Database 는 사용자 개입 없이 업그레이드, 패치, 백업, 모니터링 같은 대부분의 데이터베이스 관리 기능을 처리하는 완전 관리형 PaaS(Platform as a Service) 데이터베이스 엔진입니다.</td></tr>
<tr><td>Azure SQL
(SQL Managed Instance)</td><td>Azure SQL Managed Instance 는 확장 가능한 지능형 클라우드 데이터베이스 서비스로, 완전히 관리되는 서비스형 에버그린 플랫폼의 모든 이점에 가장 광범위한 SQL Server 데이터베이스 엔진 호환성을 결합했습니다.</td></tr>
<tr><td>SQL Server</td><td>Azure SQL 은 Azure 클라우드에서 SQL Server 데이터베이스 엔진을 사용하는 관리형, 보안 및 인텔리전트 제품군입니다.</td></tr>
<tr><td rowspan="2">데이터 암호화</td><td>Azure Cosmos DB</td><td>완전 관리형 서비스인 Azure Cosmos DB 는 자동 관리, 업데이트 및 패치를 통해 데이터베이스 관리를 직접 수행할 수 있습니다. 또한 용량과 비용을 일치시키기 위해 애플리케이션 요구 사항에 대응하는 비용 효율적인 서버리스 및 자동 확장 옵션으로 용량 관리를 처리합니다.</td></tr>
<tr><td>Azure
(SQL 가상 머신)</td><td>Azure Virtual Machines 의 SQL Server 를 사용하면 온-프레미스 하드웨어를 관리할 필요 없이 클라우드에서 SQL Server 의 전체 버전을 사용할 수 있습니다.</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 투명한 데이터 암호화 (TDE) 설정 방법
1) SQL 데이터베이스 메뉴 내 데이터 암호화 (TDE)를 설정할 데이터베이스 선택</td></tr>
</table>

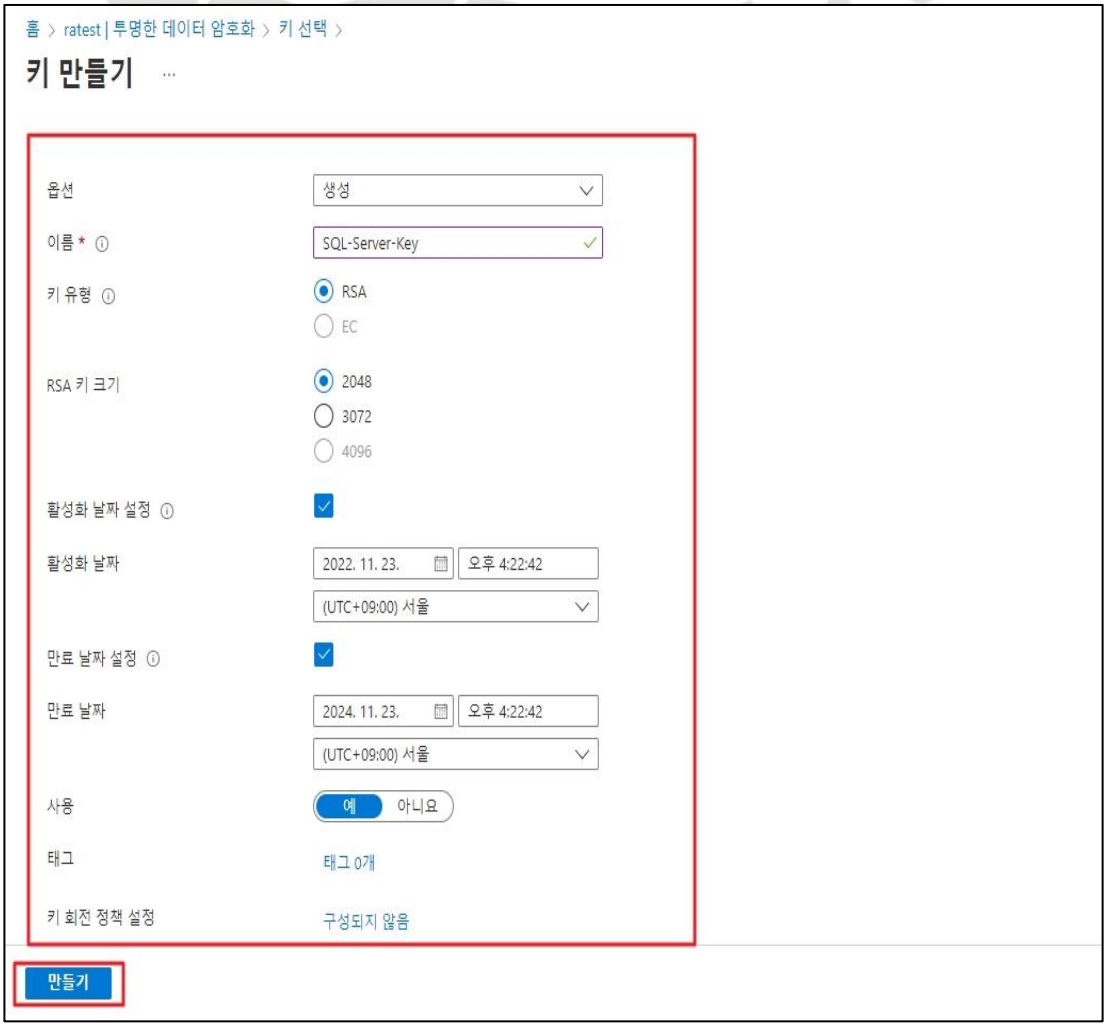
2) 투명한 데이터 암호화 메뉴 내 데이터 암호화 설정 및 저장 후 암호화 상태 확인

3) SQL 서버 메뉴 내 데이터 암호화(TDE)를 설정할 SQL 서버 선택

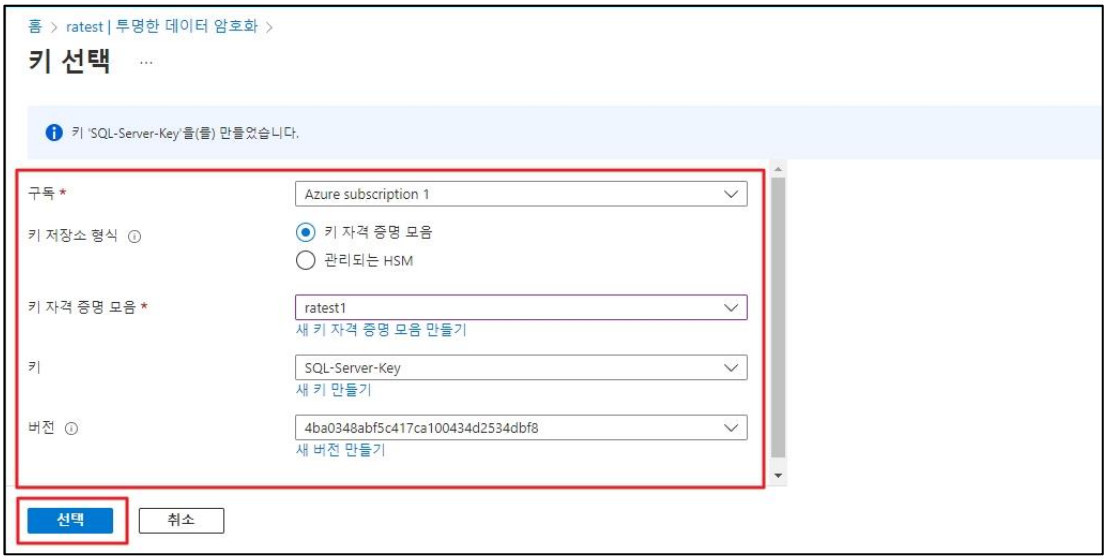
4) 투명한 데이터 암호화 메뉴 내 고객 관리형 키 사용 옵션 설정

5) 암호화에 사용할 새 키 만들기

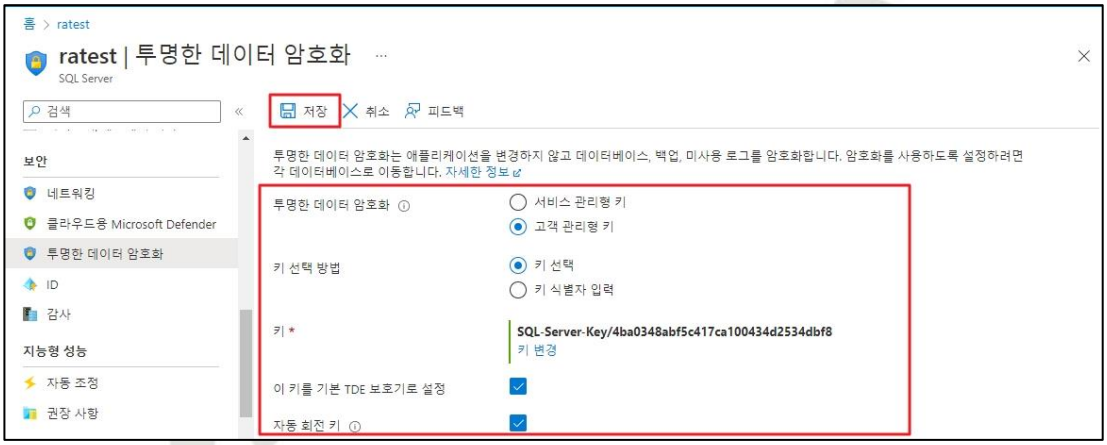




6) 사용할 암호화 키 선택

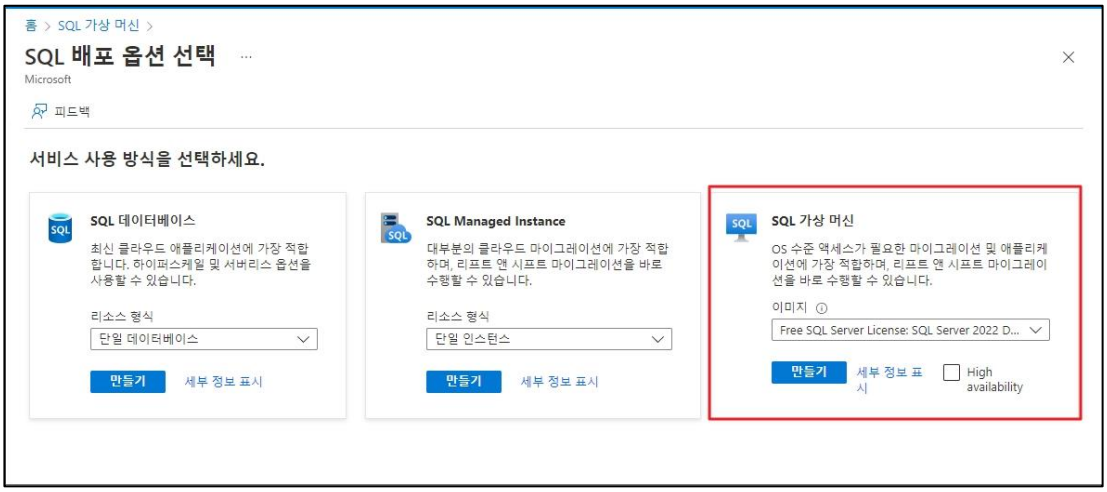


7) 암호화 설정 및 저장

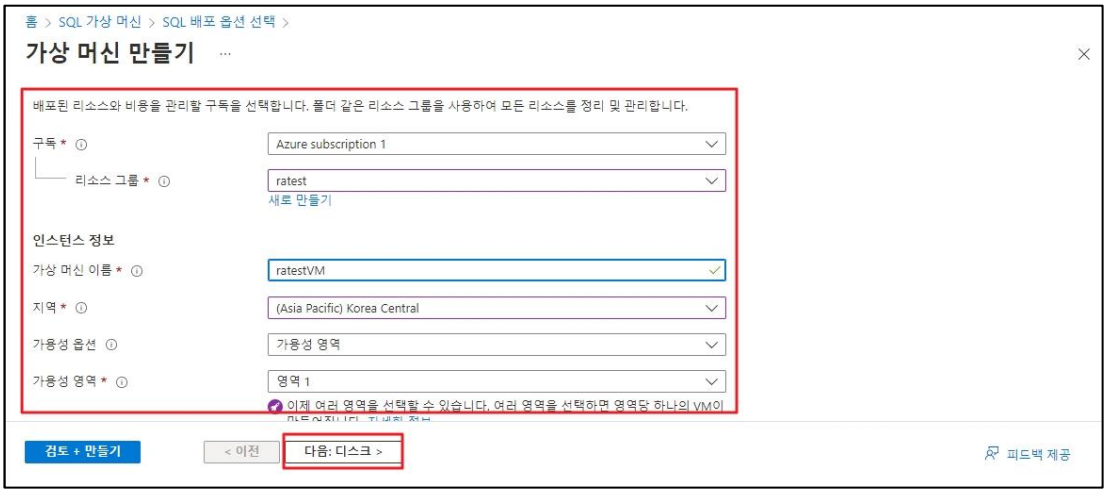


나. 데이터 암호화 설정 방법

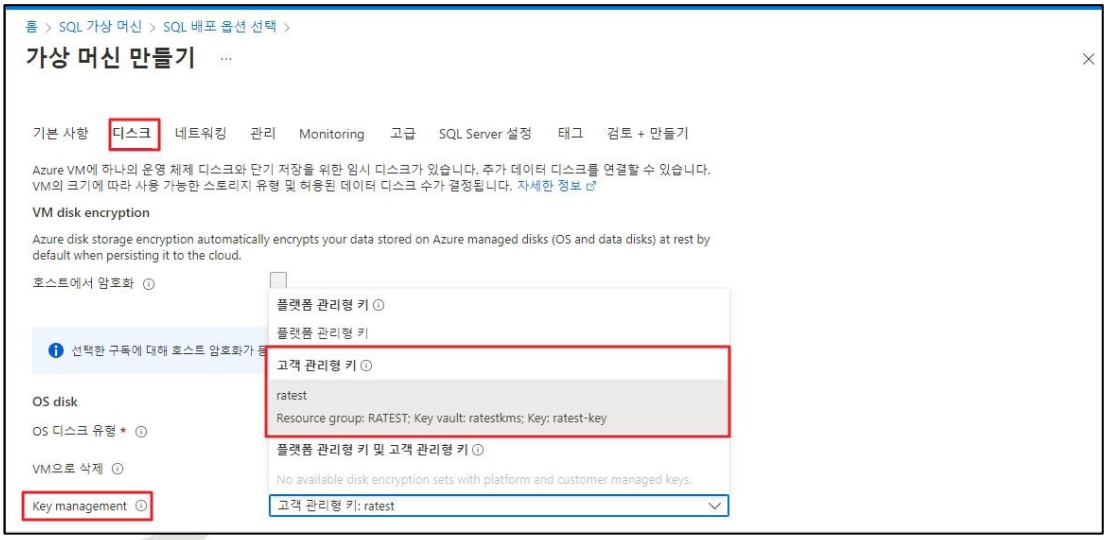
1) SQL 가상 머신 메뉴 내 이미지 선택



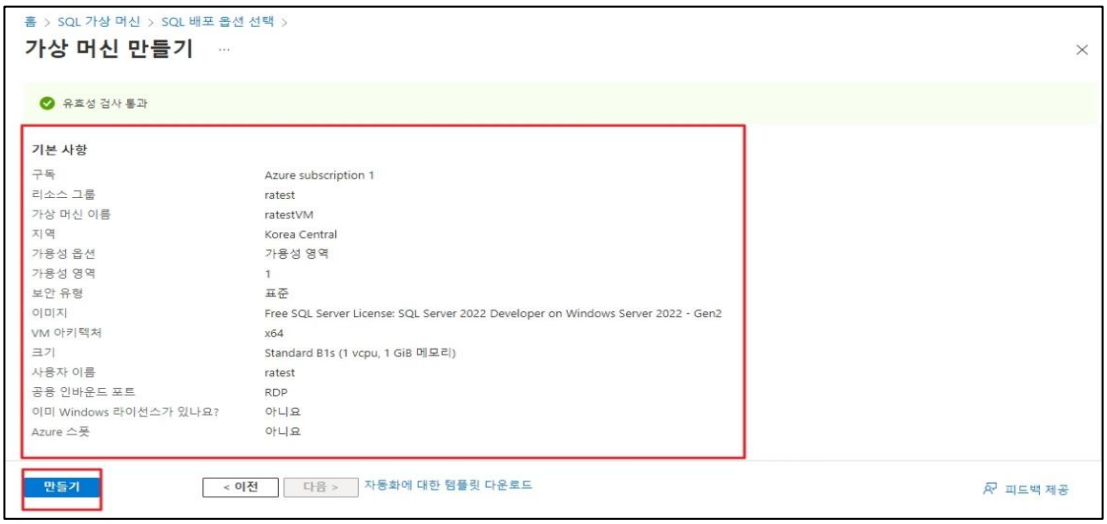
2) 가상 머신 만들기 메뉴 내 기본사항 정보 입력



3) 디스크 메뉴 내 고객 관리형 키 선택



4) 투명한 데이터 암호화 메뉴 내 고객 관리형 키 사용 옵션 설정

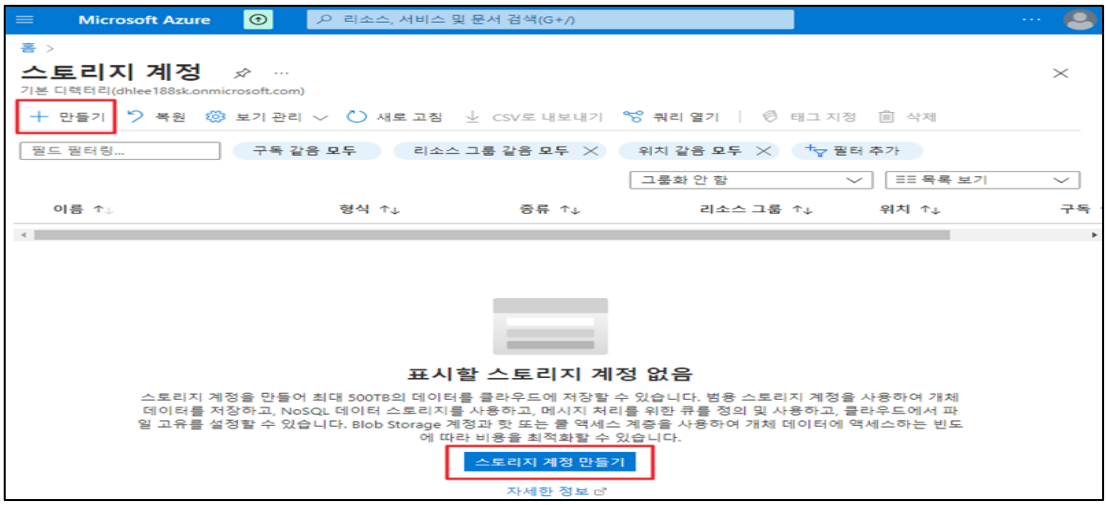


진단 기준	**양호기준** : 투명한 데이터 암호화 및 데이터 암호화 기능이 설정되어 있을 경우 **취약기준** : 투명한 데이터 암호화 및 데이터 암호화 기능이 설정되어 있지 않을 경우
비고	

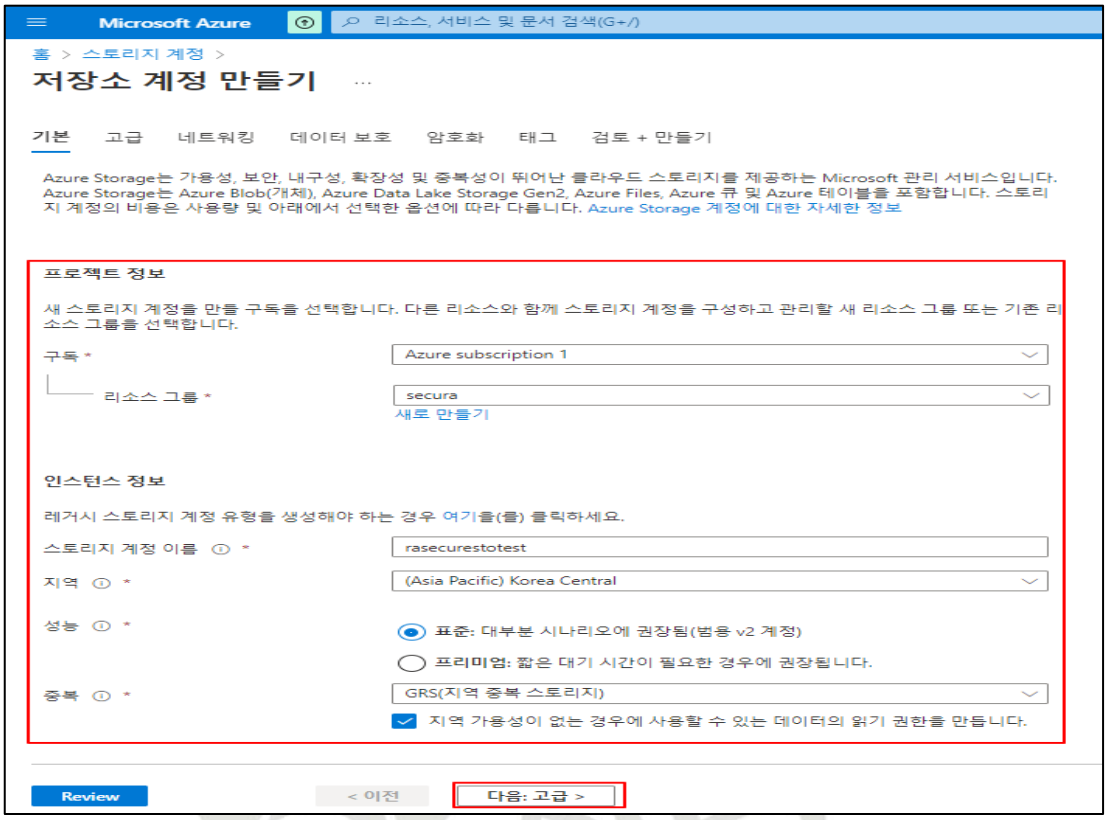
4.2 스토리지 암호화 설정

<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">스토리지 암호화 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">키 자격 증명 모음(Key Vault)은 "비밀 관리(토큰, 암호, 인증서 제어)", "키 관리(데이터 암호화)", "인증서 관리(퍼블릭/프라이빗 SSL/TLS 인증서 프로비저닝, 배포 관리)"등으로 활용될 수 있으며 스토리지 계정의 암호화는 리소스 관리자 및 클래식 저장소 계정을 포함하여 모든 저장소 계정에 대해 사용하도록 설정되며, AES 256 암호화 방식을 채택하고 있습니다.

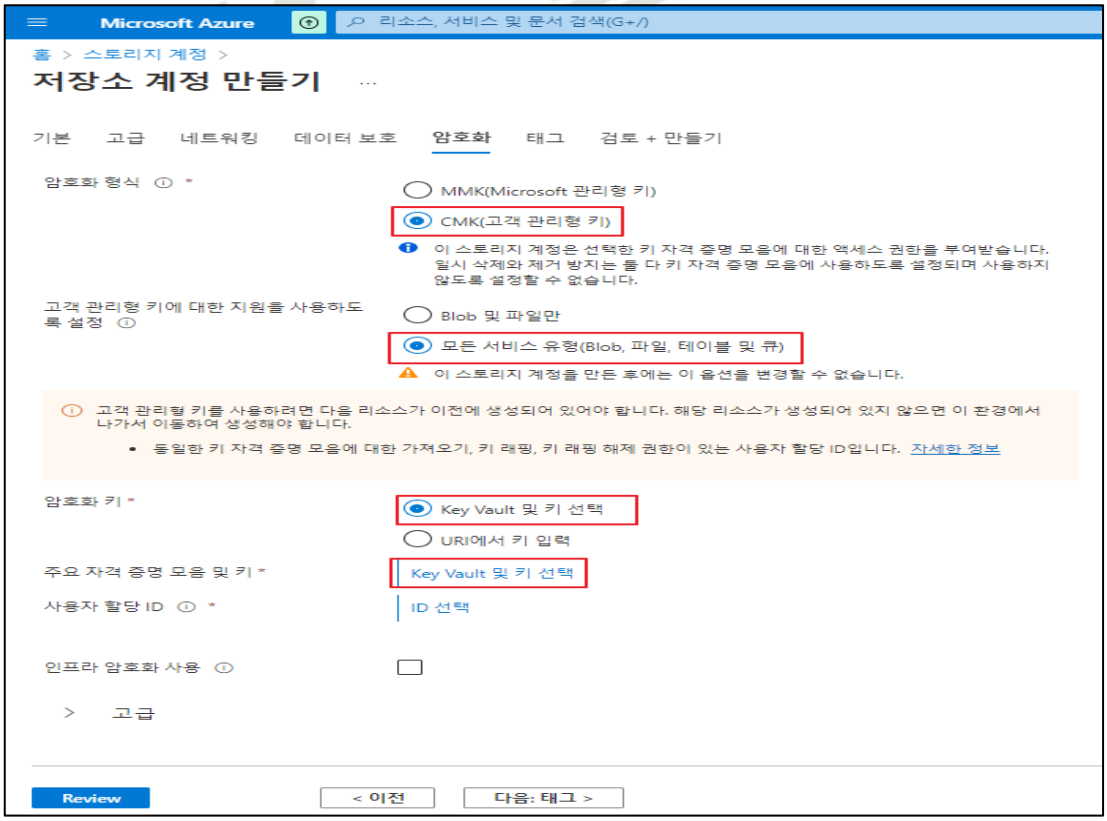
암호화 적용 방식은 "Microsoft 관리형 키", "고객 관리형 키" 두 가지로 나뉘어 지며 방식은 어떤 것을 사용하여도 암호화 적용은 되지만 "고객 관리형 키"의 경우는 키 자격 증명 모음(Key Vault)을 통해 키를 별도로 생성하여 접근 권한, 키 만료 일자, 액세스 제어(IAM)등의 설정이 가능해 집니다. 서비스 운영자/관리자는 "서비스 관리형 키", "고객 관리형 키" 둘 중 하나를 선택하여 적용해도 되지만, "고객 관리형 키"의 경우 키에 대한 만료 일자를 주기적으로 변경해야 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지 할 수 있습니다.

(*) 암호화 키 관리 옵션
<table>
<tr><th>키 관리 매개 변수</th><th>Microsoft
관리형 키</th><th>고객 관리형 키</th><th>고객이 제공한 키</th></tr>
<tr><td>암호화/암호 해독 작업</td><td>Azure</td><td>Azure</td><td>Azure</td></tr>
<tr><td>지원되는 Storage 서비스</td><td>모두</td><td>Blob, Files</td><td>Blob</td></tr>
<tr><td>키 스토리지</td><td>Microsoft 키 저장소</td><td>Key valut 또는 HSM</td><td>고객의 고유 키 저장소</td></tr>
<tr><td>키 회전 책임</td><td>Microsoft</td><td>Customer</td><td>Customer</td></tr>
<tr><td>키 컨트롤</td><td>Microsoft</td><td>Customer</td><td>Customer</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 스토리지 계정 생성 및 암호화 설정
1) 스토리지 계정 만들기
 
</td></tr>
</table>

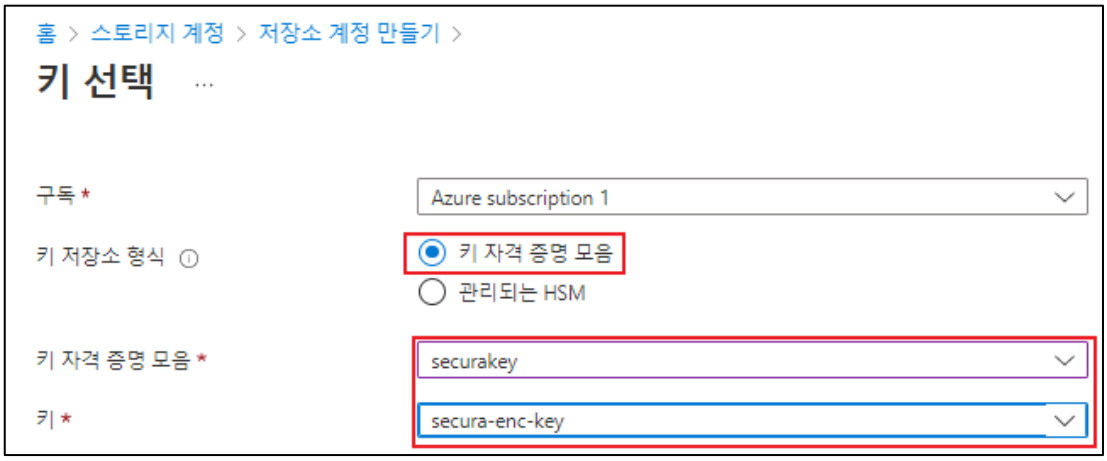
2) 스토리지 계정 기본 사항 입력



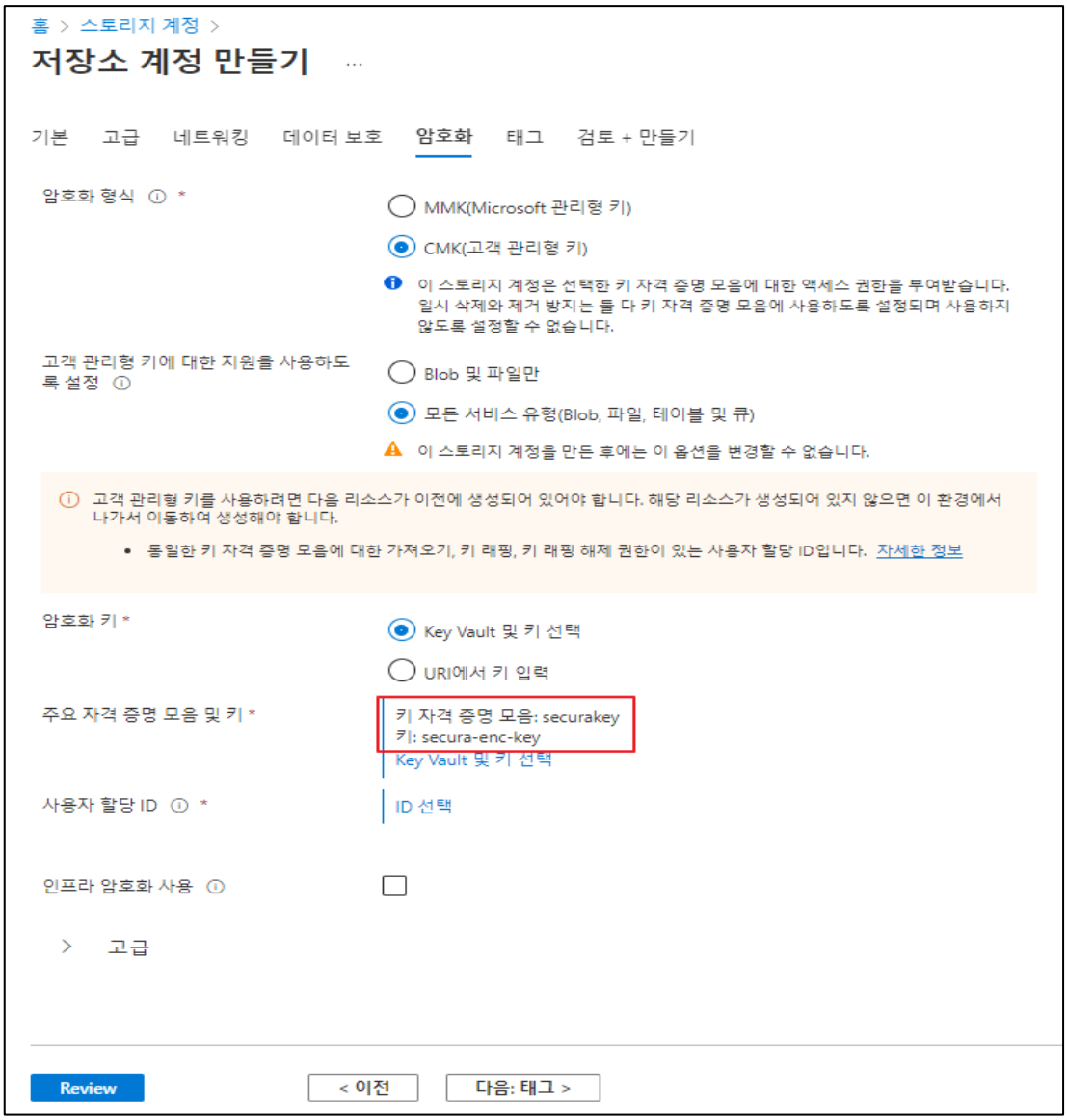
3) 스토리지 계정 암호화 설정



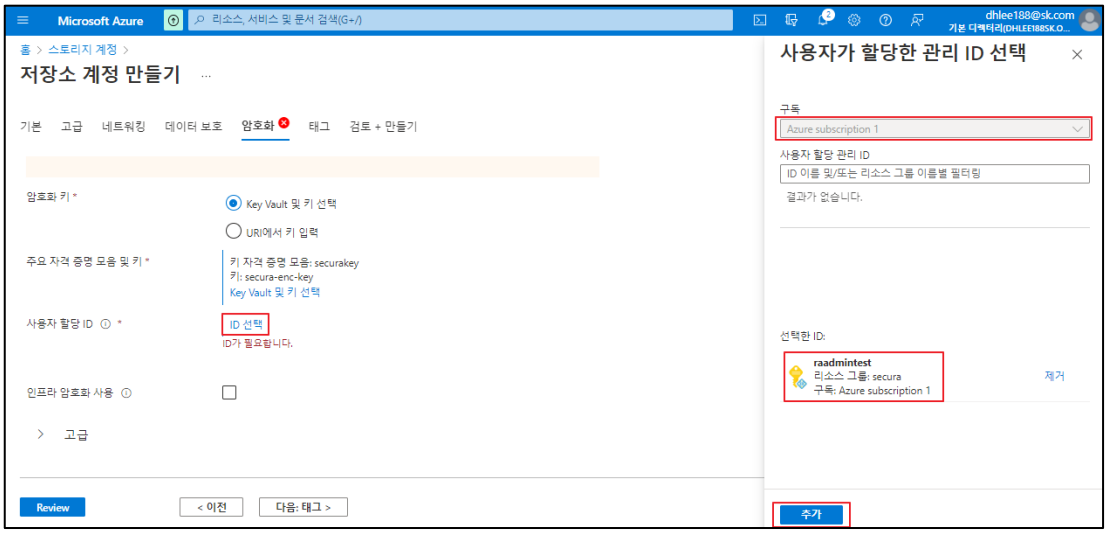
4) Azure key Vault 키 자격 모음 선택



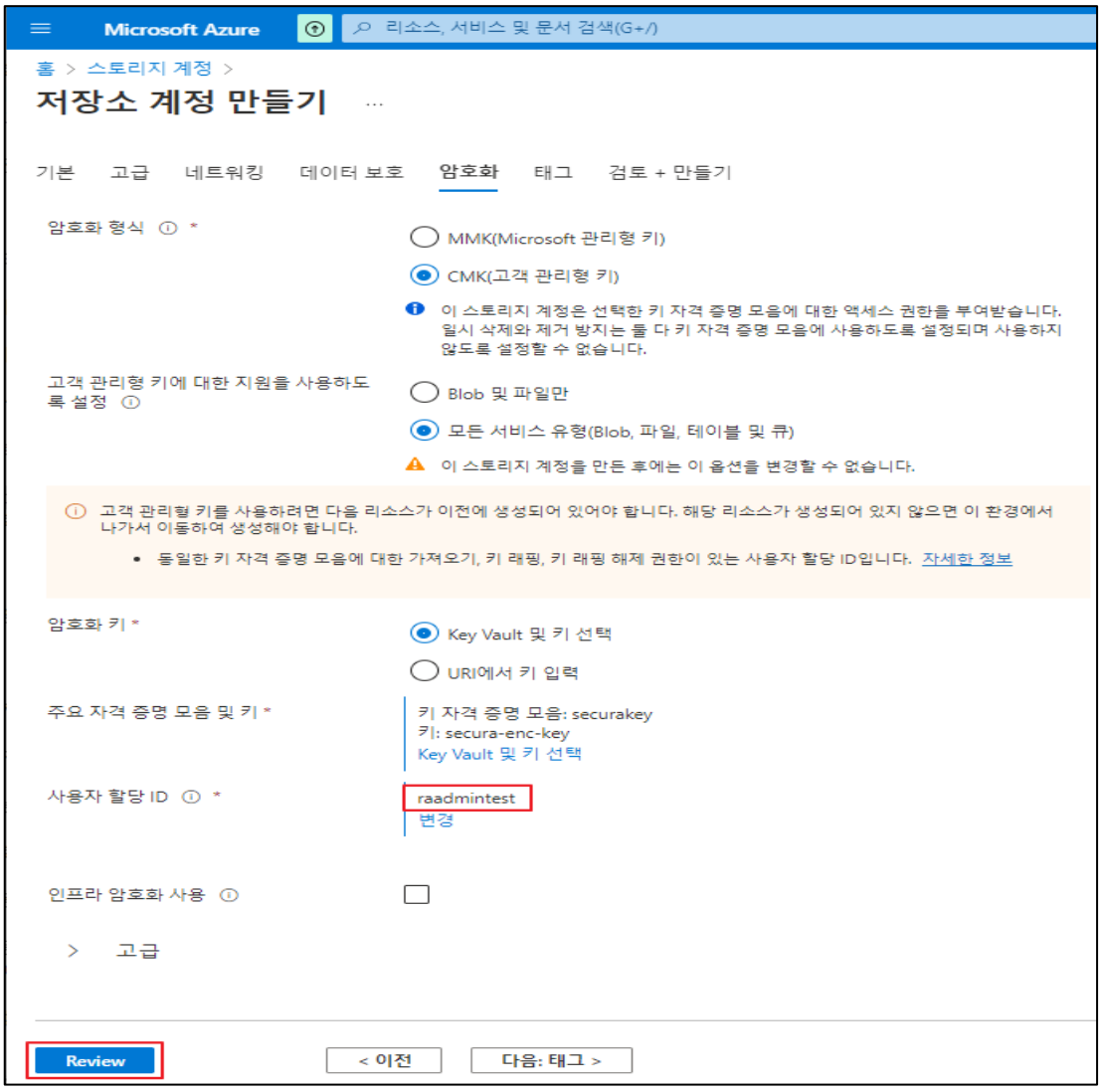
5) Azure key Vault 키 자격 모음 선택 후 등록



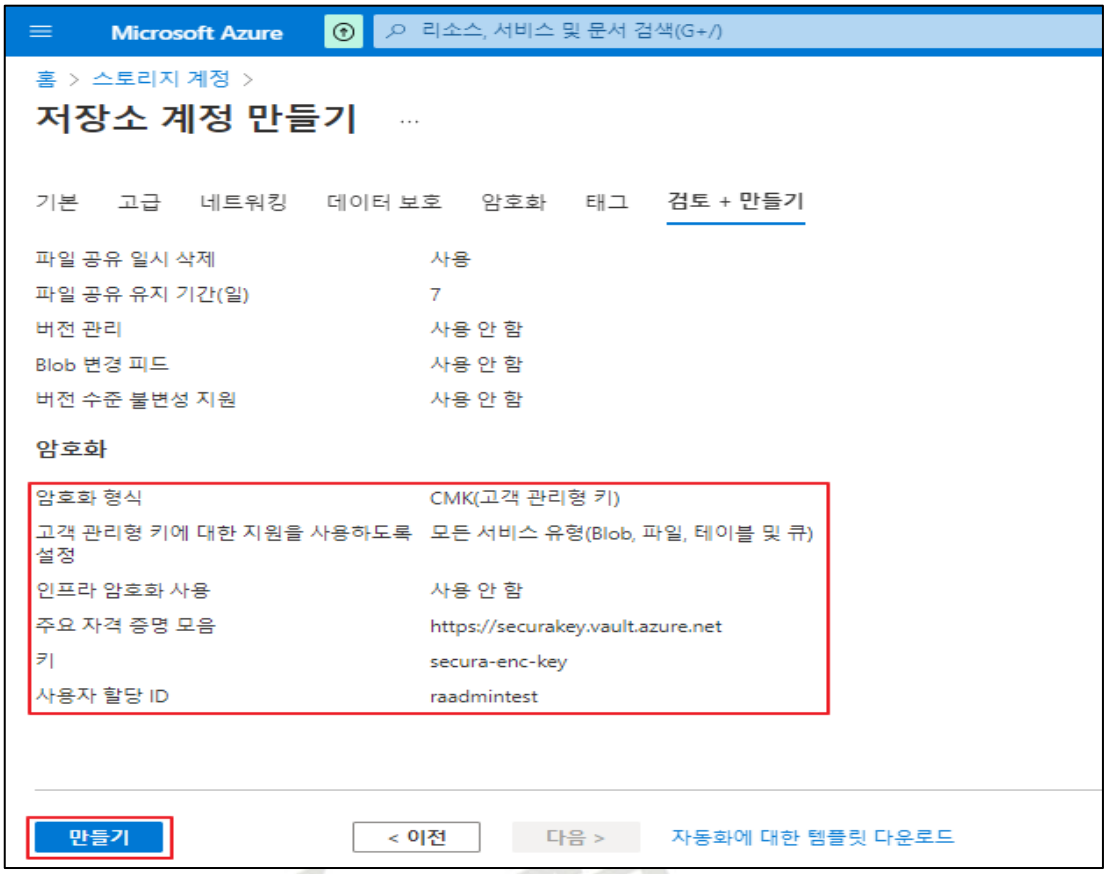
6) 사용자 할당 ID 선택



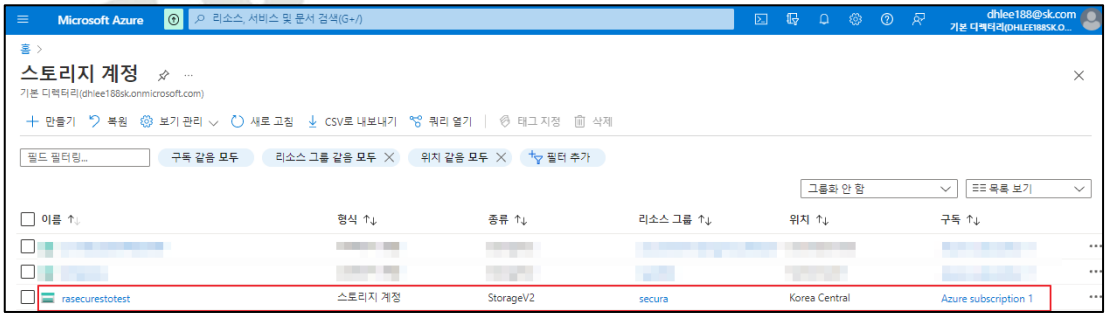
7) 관리ID 등록



8) 스토리지 계정 만들기



9) 스토리지 계정 생성 완료



진단 기준

양호기준

: 사용자 고유키 및 관리형 키를 통해 암호화를 설정하고 있을 경우

취약기준

: 사용자 고유키 및 관리형 키를 통해 암호화를 설정하고 있지 않을 경우

비고

4.3 디스크 암호화 설정

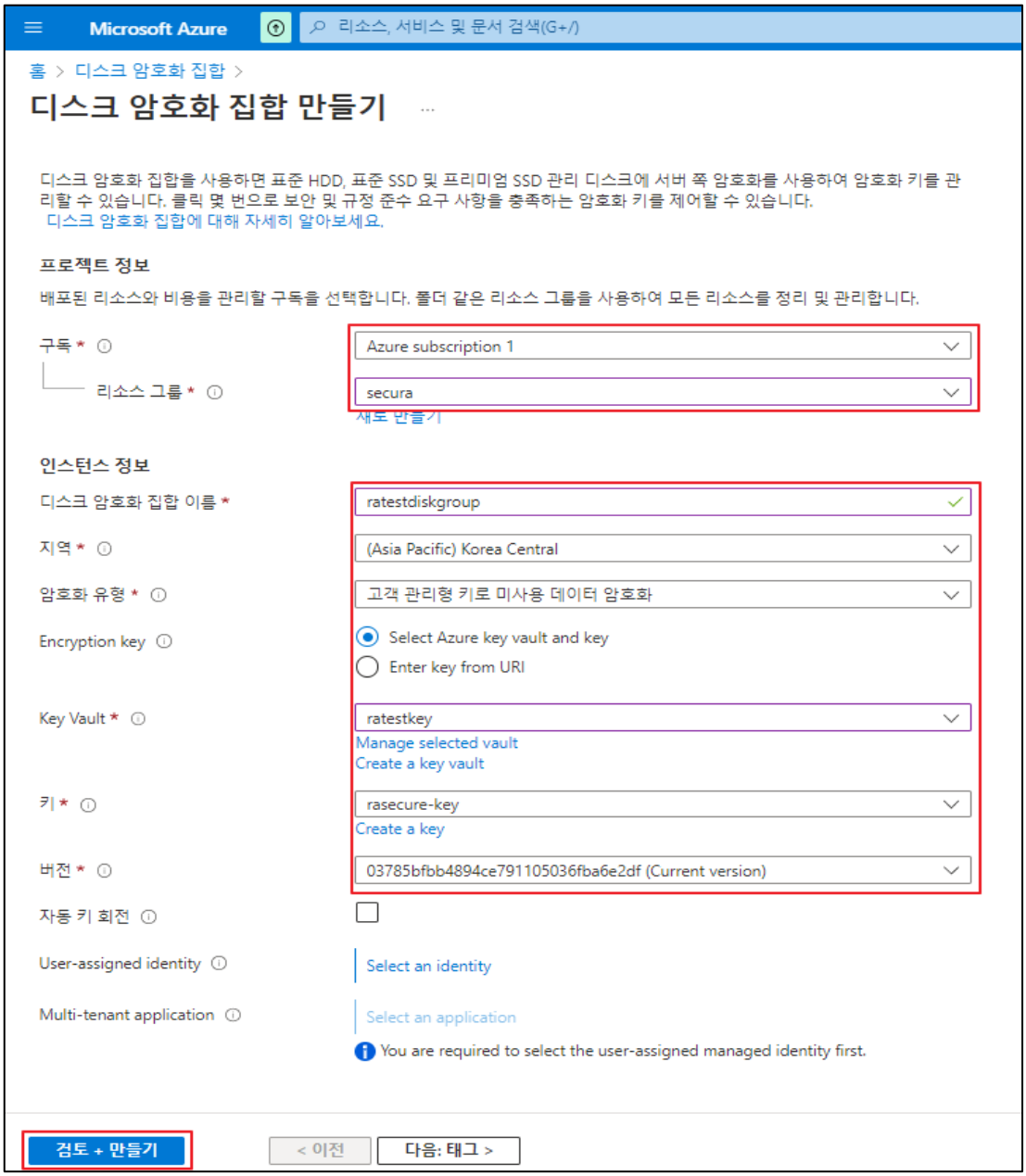
<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">디스크 암호화 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure 관리 디스크는 Azure에서 관리하고 Azure Virtual Machines와 함께 사용되는 블록 수준 스토리지 볼륨입니다. 관리 디스크는 온-프레미스 서버의 물리적 디스크와 유사하지만 가상화 되어 있습니다.

키 자격 증명 모음(Key Vault)은 "비밀 관리(토큰, 암호, 인증서 제어)", "키 관리(데이터 암호화)", "인증서 관리(퍼블릭/프라이빗 SSL/TLS 인증서 프로비저닝, 배포 관리)"등으로 활용될 수 있으며 스토리지 계정의 암호화는 리소스 관리자 및 클래식 저장소 계정을 포함하여 모든 저장소 계정에 대해 사용하도록 설정되며, AES 256 암호화 방식을 채택하고 있습니다.

암호화 적용 방식은 "Microsoft 관리형 키", "고객 관리형 키" 두 가지로 나뉘어 지며 방식은 어떤 것을 사용하여도 암호화 적용은 되지만 "고객 관리형 키"의 경우는 키 자격 증명 모음(Key Vault)을 통해 키를 별도로 생성하여 접근 권한, 키 만료 일자, 액세스 제어(IAM)등의 설정이 가능해 집니다. 서비스 운영자/관리자는 "서비스 관리형 키", "고객 관리형 키" 둘 중 하나를 선택하여 적용해도 되지만, "고객 관리형 키"의 경우 키에 대한 만료 일자를 주기적으로 변경해야 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지 할 수 있습니다.

(*) 암호화 키 관리 옵션
<table>
<tr><th>키 관리 매개 변수</th><th>Microsoft
관리형 키</th><th>고객 관리형 키</th><th>고객이 제공한 키</th></tr>
<tr><td>암호화/암호 해독 작업</td><td>Azure</td><td>Azure</td><td>Azure</td></tr>
<tr><td>지원되는 Storage 서비스</td><td>모두</td><td>Blob, Files</td><td>Blob</td></tr>
<tr><td>키 스토리지</td><td>Microsoft 키 저장소</td><td>Key valut 또는 HSM</td><td>고객의 고유 키 저장소</td></tr>
<tr><td>키 회전 책임</td><td>Microsoft</td><td>Customer</td><td>Customer</td></tr>
<tr><td>키 컨트롤</td><td>Microsoft</td><td>Customer</td><td>Customer</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 디스크 암호화 집합 설정
1) 디스크 암호화 집합 만들기
 
</td></tr>
</table>

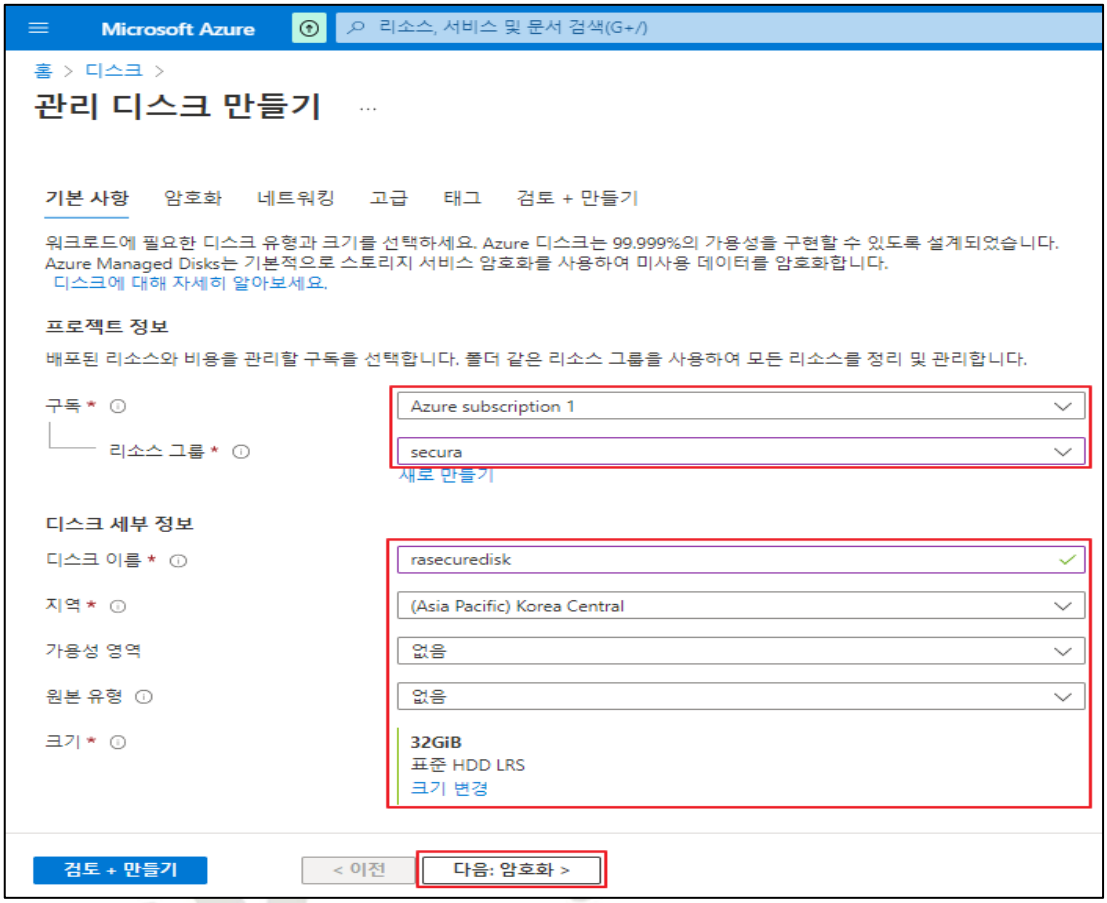
2) 디스크 암호화 집합 내 기 생성 완료 된 Key Vault 선택 후 생성



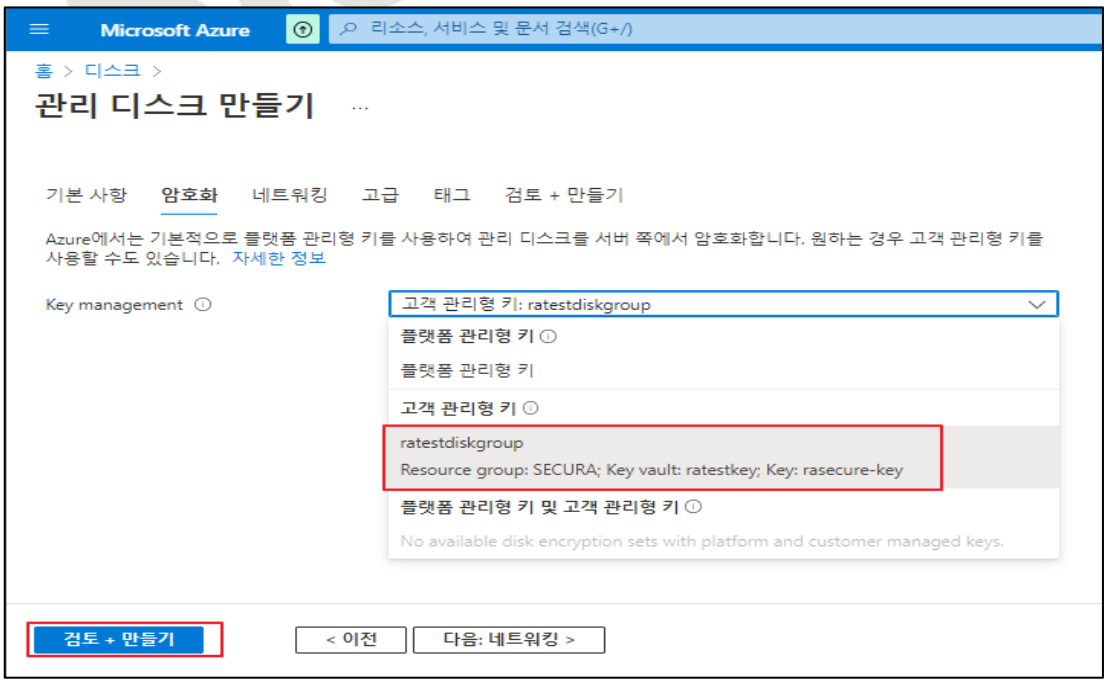
3) 디스크 암호화 집합 생성 완료

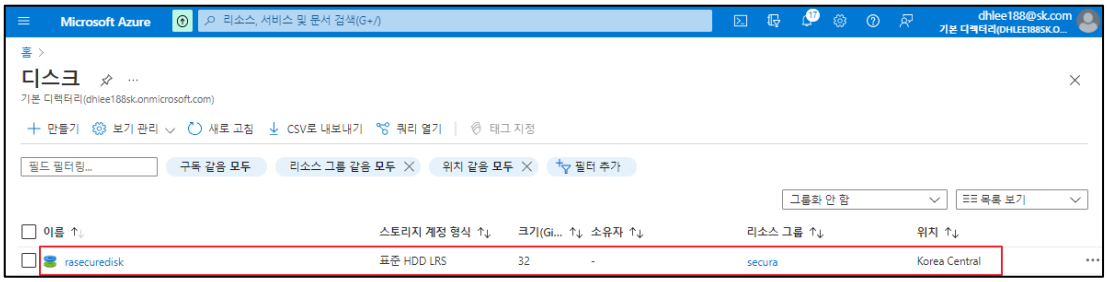
나. 디스크 생성 및 암호화 설정

1) 디스크 만들기 내 기본 사항 입력



2) 디스크 암호화 고객 관리형 키 선택



	3) 디스크 생성 완료 
진단 기준	**양호기준** : 플랫폼 관리형 키 및 고객 관리형 키를 통해 암호화를 설정하고 있을 경우 **취약기준** : 플랫폼 관리형 키 및 고객 관리형 키를 통해 암호화를 설정하고 있지 않을 경우
비고	

4.4 통신구간 암호화 설정

<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">통신구간 암호화 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">클라우드 리소스를 통해 대/내외 서비스에서 정보를 송, 수신하는 경우 중간에서 공격자가 패킷을 가로채어 공격에 활용할 수 없도록 통신 구간을 암호화하여 설정하여야 합니다.</td></tr>
<tr><td>설정
방법</td><td colspan="3">
가. 중요정보 전송 시 암호화 정책 수립
1) 중요정보 전송 시 이동 구간 암호화
- 암호화된 통신 채널 사용
- 서버 원격 접근 시 암호화된 통신수단(VPN, SSH등)을 사용
- 공공기관 데이터 이관 시 VPN을 통해 이관
- 기타 관리를 위한 접근 시 OpenSSH 및 OpenSSL(TLS V1.2) 사용

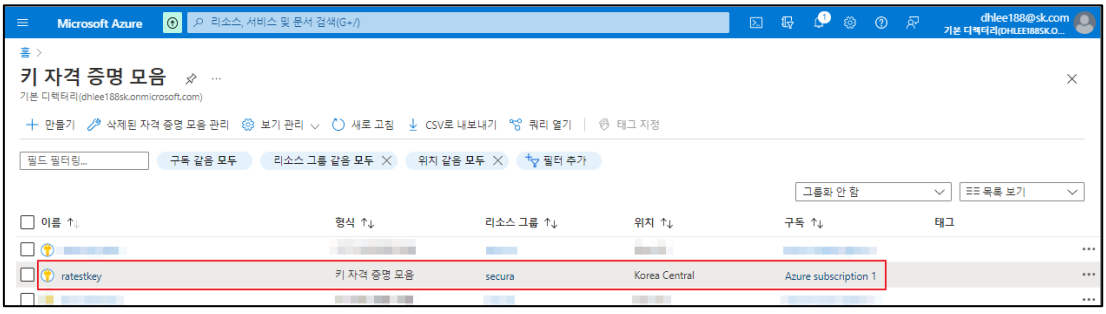
(*) 중요정보 전송 및 저장 시 암호화 방안 예시
<table>
<tr><th>구분</th><th>암호화 방안</th></tr>
<tr><td>서버와 클라이언트 간 전송</td><td>SSL 방식
응용프로그램</td></tr>
<tr><td>개인정보처리시스템 간 전송</td><td>IPSec 방식, SSL 방식, SSH 방식</td></tr>
<tr><td>개인정보처리시스템 암호화 방식</td><td>응용프로그램 자체 암호화
DB 서버 암호화
DBMS 자체 암호화
DBMS 암호화 기능 호출
운영체제 암호화</td></tr>
<tr><td>업무용 컴퓨터
보조저장매체 암호화 방식</td><td>문서 도구 자체 암호화
암호 유틸리티 이용 암호화
DRM
디스크 암호화</td></tr>
</table>
※ 클라우드서비스 보안인증제도(IaaS) 평가기준 해설서의 “11.1.4 네트워크 암호화 및 12.3.1 암호 정책 수립” 항목 참고
</td></tr>
<tr><td>진단
기준</td><td colspan="3">
양호기준
: 클라우드 리소스 통신 구간 내 암호화 설정이 되어 있는 경우

취약기준
: 클라우드 리소스 통신 구간 내 암호화 설정이 되어 있지 않는 경우
</td></tr>
<tr><td>비고</td><td colspan="3"></td></tr>
</table>

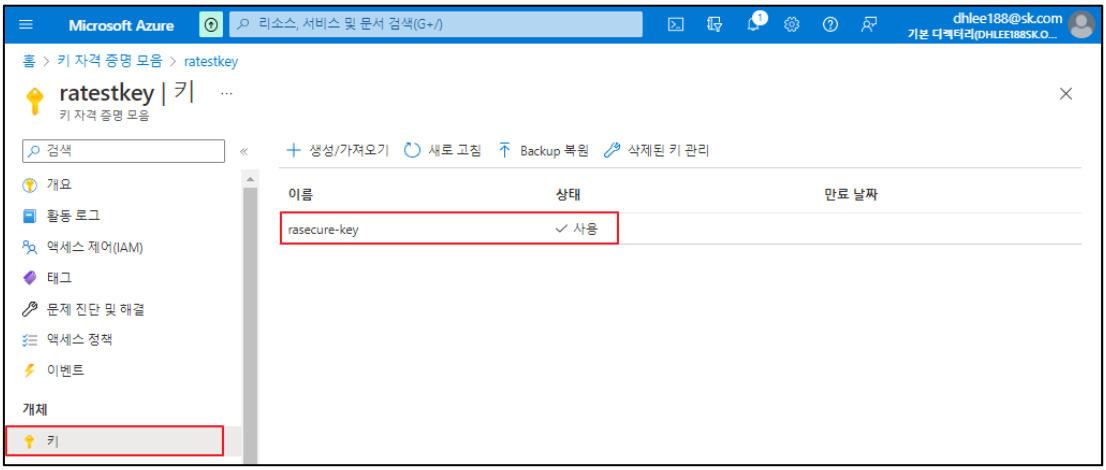
4.5 키 자격 증명 모음 회전 정책 관리

<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">통신구간 암호화 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">Key Vault에서 암호화 키 순환을 자동화하면 사용자는 지정된 빈도에 따라 새로운 키 버전을 자동으로 생성하도록 Key Vault를 구성할 수 있습니다. 회전을 구성하려면 각 개별 키에 정의할 수 있는 키 회전 정책을 사용할 수 있으며 키 순환 정책을 사용하면 순환 및 Event Grid 알림의 만료 임박 알림을 구성할 수 있습니다.

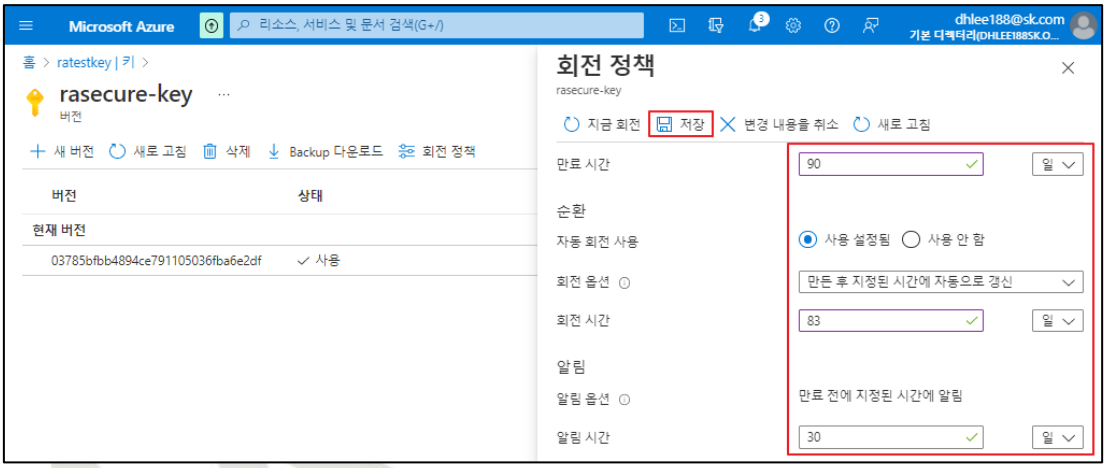
키 순환은 새 키 자료를 사용하여 기존 키의 새 키 버전을 생성합니다. 대상 서비스는 버전 없는 키 URI를 사용하여 최신 버전의 키로 자동으로 새로 고쳐야 합니다. 데이터 암호화 솔루션이 암호 해독/래핑 해제 작업에 대해 암호화/래핑 작업에 사용된 것과 같은 키 자료를 가리키는 데이터와 함께 버전이 지정된 키 URI를 저장하도록 하여 서비스 중단을 방지합니다. 모든 Azure 서비스는 현재 데이터 암호화에 대해 해당 패턴을 따르고 있습니다.

※ 회전 정책 옵션
<table>
<tr><th>구분</th><th>상세내용</th></tr>
<tr><td>만료 시간</td><td>키 만료 간격입니다. 새로 순환된 키의 만료 날짜를 설정하는 데 사용됩니다. 현재 키에는 영향을 주지 않습니다.</td></tr>
<tr><td>자동 회전 사용</td><td>키 회전을 사용하거나 사용하지 않도록 설정하는 플래그
ex. 사용/사용 안 함</td></tr>
<tr><td>회전 옵션</td><td>키를 만든 후 지정된 시간에 자동으로 갱신(기본값)
만료 전에 지정된 시간에 자동으로 갱신. 회전 정책에서 '만료 시간'을 설정하고 키에서 '만료 날짜'를 설정해야 합니다.</td></tr>
<tr><td>회전 시간</td><td>키 순환 간격. 최솟값은 생성 후 7일 및 만료 시간으로부터 7일입니다.</td></tr>
<tr><td>알림 옵션</td><td>만료 이벤트가 임박한 키의 이벤트 그리드 알림 간격입니다. 회전 정책에서 '만료 시간'을 설정하고 키에서 '만료 날짜'를 설정해야 합니다.</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 키 자격 증명 모음 회전 정책 설정
1) 키 자격 증명 모음 확인 및 선택
 
</td></tr>
</table>

2) 키 자격 증명 모음 키 개체 확인 및 선택



3) 키 회전 정책 설정 (만료시간, 자동회전 활성화, 회전 시간, 알림 시간)



4) 키 회전 정책 적용 완료

진단 기준

양호기준

: 사용자 고유키에 대한 회전 정책이 기준(90일)에 맞게 설정되어 있을 경우

취약기준

: 사용자 고유키에 대한 회전 정책이 기준(90 일 초과)에 맞게 설정되어 있지 않을 경우

비고

4.6 AD 감사 로그 설정

<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">AD 감사 로그 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">
Azure AD 내의 다양한 기능에 의해 수행된 모든 변경 내용에 대한 로그를 통해 추적 기능을 제공합니다. 감사 로그의 예제로는 사용자, 앱, 그룹, 역할 및 정책 추가 또는 제거와 같은 Azure AD 내의 모든 리소스에 대한 변경 내용이 있습니다.

감사 로그는 일반 사용자도 자신의 감사 로그를 확인할 수 있으나, 게스트 계정은 별도 관리자 권한을 부여 받지 않는 이상 감사 로그를 확인할 수 없습니다. 기본적으로 제한적 권한을 갖는 게스트 사용자 계정은 최소권한으로 최소기간으로 사용되어야 하므로, 관리자 권한이 부여되지 않도록 주의해야 합니다.

※ 필수 감사 로그 범주: “AuditLogs, SignInLogs, RiskyUsers, UserRiskEvents”
최소 보관 기간: 1 년

※ 회전 정책 옵션
<table>
<tr><th>구분</th><th>상세내용</th></tr>
<tr><td>AuditLogs</td><td>Azure Active Directory의 감사 로그입니다. 사용자 및 그룹 관리, 관리형 애플리케이션, 디렉터리 작업에 대한 시스템 작업 정보를 포함합니다.</td></tr>
<tr><td>SignInLogs</td><td>서비스 주체 Azure Active Directory 로그인 로그</td></tr>
<tr><td>NonInteractive UserSignInLogs</td><td>사용자의 비대화형 Azure Active Directory 로그인 로그.</td></tr>
<tr><td>ServicePrincipal SignInLogs</td><td>서비스 주체 Azure Active Directory 로그인 로그</td></tr>
<tr><td>ManagedIdentity SignInLogs</td><td>관리 ID Azure Active Directory 로그인 로그</td></tr>
<tr><td>ProvisioningLogs</td><td>Azure AD 프로비저닝에서 생성된 로그</td></tr>
<tr><td>ADFSSignInLogs</td><td>Active Directory Federation Service에서 생성된 로그</td></tr>
<tr><td>RiskyUsers</td><td>Azure AD 위험한 사용자에 대한 ID 보호에서 생성된 로그</td></tr>
<tr><td>UserRiskEvents</td><td>Azure AD 사용자 위험 이벤트에 대한 ID 보호에서 생성된 로그</td></tr>
<tr><td>NetworkAccess TrafficLogs</td><td>이 테이블은 네트워크 트래픽 액세스 로그를 포함하는 ID 및 네트워크 액세스의 일부입니다. 이러한 로그는 정책, 위험 및 트래픽 관리에 활용될 뿐만 아니라 사용자 환경을 모니터링할 수 있습니다.</td></tr>
<tr><td>RiskyService Principals</td><td>Azure AD 위험한 서비스 주체에 대한 ID 보호에 의해 생성된 로그</td></tr>
<tr><td>ServicePrincipal RiskEvents</td><td>Azure AD 서비스 주체 위험 이벤트에 대한 ID 보호에 의해 생성된 로그</td></tr>
</table>

※ 로그 전달 대상
</td></tr>
</table>

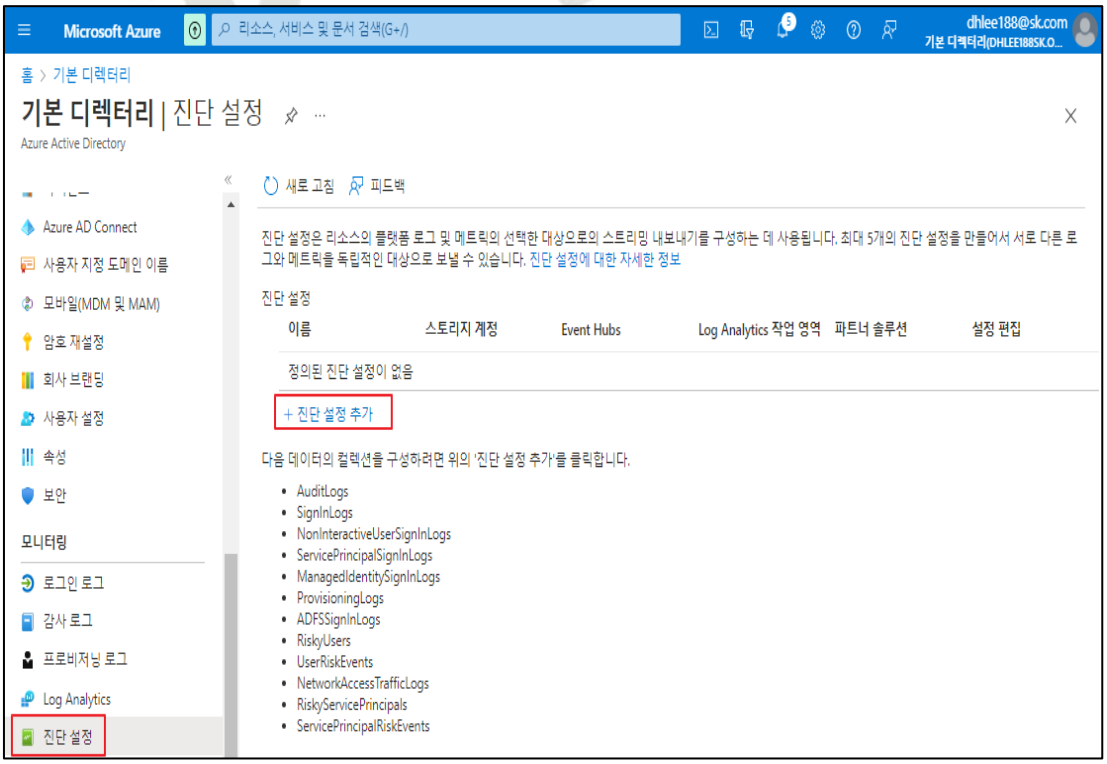
구분	상세 내용
로그 분석 작업 영역	메트릭은 로그 형식으로 변환됩니다. 이 옵션은 모든 리소스 종류에 사용할 수 있는 것은 아닙니다. Azure Monitor 로그 저장소(Log Analytics를 통해 검색 가능)로 보내면 기존 로그 데이터를 사용하여 쿼리, 경고 및 시각화에 통합하는 데 도움이 됩니다.
Azure 저장소 계정	로그 및 메트릭을 Storage 계정에 보관하는 것은 감사, 정적 분석 또는 백업에 유용합니다. Azure Monitor 로그 또는 로그 분석 작업 영역을 사용하는 것과 비교할 때 저장소는 비용이 저렴하며 로그를 무기한 보관할 수 있습니다.
Azure Event Hubs	이벤트 허브에 로그 및 메트릭을 보낼 때 타사 SIEM 및 기타 Log Analytics 솔루션과 같은 외부 시스템으로 데이터를 스트리밍할 수 있습니다.
Azure 모니터 파트너 통합	Azure 모니터와 다른 타사 모니터링 플랫폼 간에 특수 통합을 수행할 수 있습니다. 통합은 파트너 중 하나를 이미 사용 중인 경우에 유용합니다.

※ AD 감사 로그는 최대 30 일간 저장되며, 더 긴 보존기간이 필요할 경우, 다운로드를 통해 별도 보관 및 관리하거나, 스토리지 계정을 통해 별도 관리가 필요합니다.

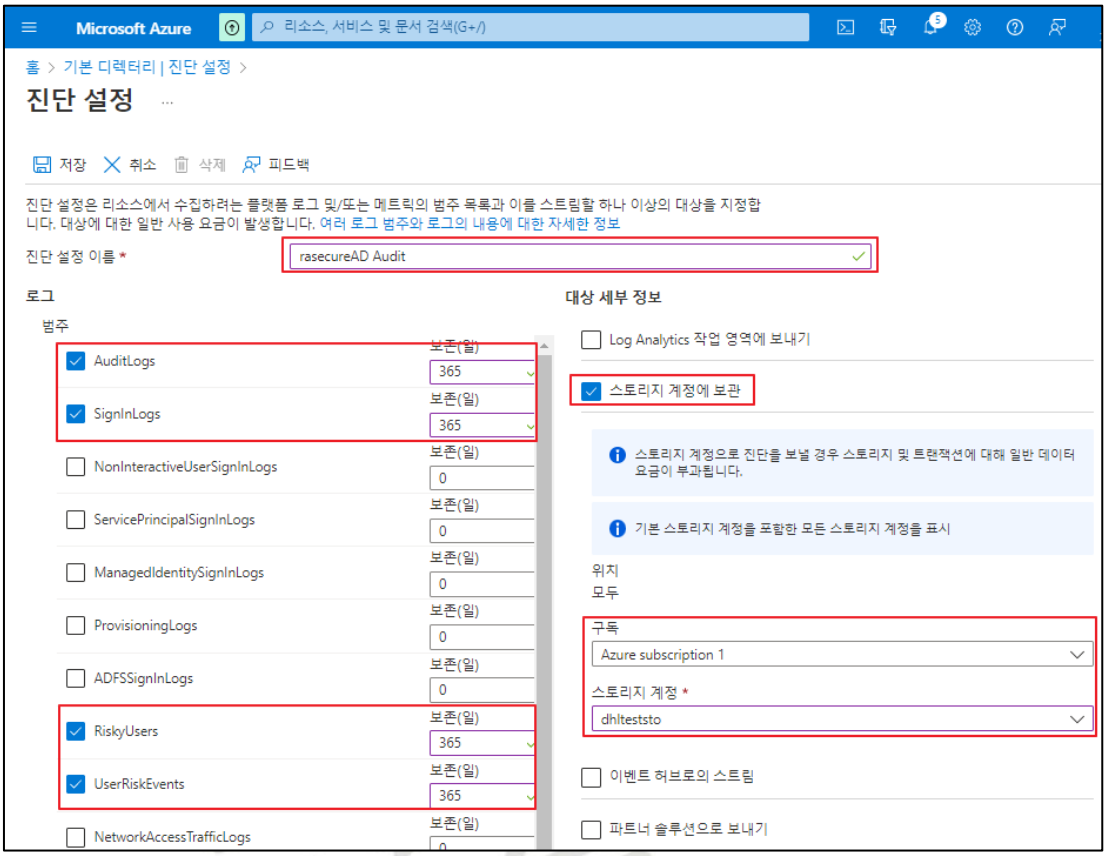
설정 방법

가. Azure AD 감사 로그 스토리지 저장 설정 방법

1) Azure Active Directory 메뉴 내 진단 설정 및 진단 설정 추가 버튼 선택



2) 진단 설정 기본 사항 및 스토리지 계정 선택 후 저장



3) 진단 설정 목록 내 정상 생성 유무 확인

진단 기준	**양호기준** : AD 감사 로그 보관 정책이 존재하고 있을 경우 **취약기준** : AD 감사 로그 보관 정책이 존재하고 있지 않을 경우
비고	

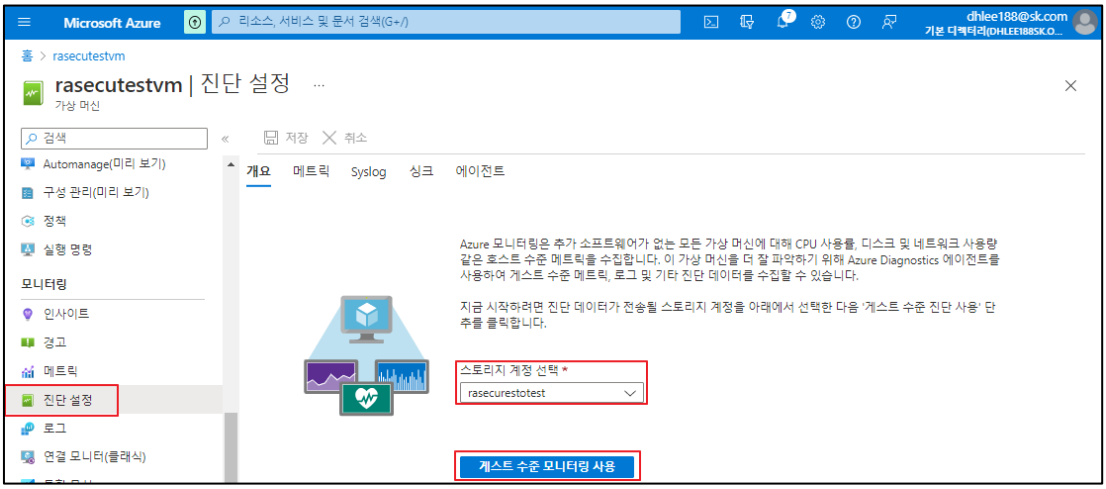
4.7 인스턴스 서비스 감사 로그 설정

<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">인스턴스 서비스 감사 로그 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure 모니터의 로그 분석 에이전트에 대한 사용자 지정 로그 데이터 원본을 사용하면 Windows 및 Linux 컴퓨터 모두의 텍스트 파일에서 이벤트를 수집할 수 있습니다. 많은 응용 프로그램은 Windows 이벤트 로그 또는 Syslog 와 같은 표준 로깅 서비스 대신 텍스트 파일에 정보를 기록합니다. 데이터가 수집된 후 쿼리의 개별 필드로 구문 분석하거나 수집하는 동안 개별 필드로 추출할 수 있습니다.

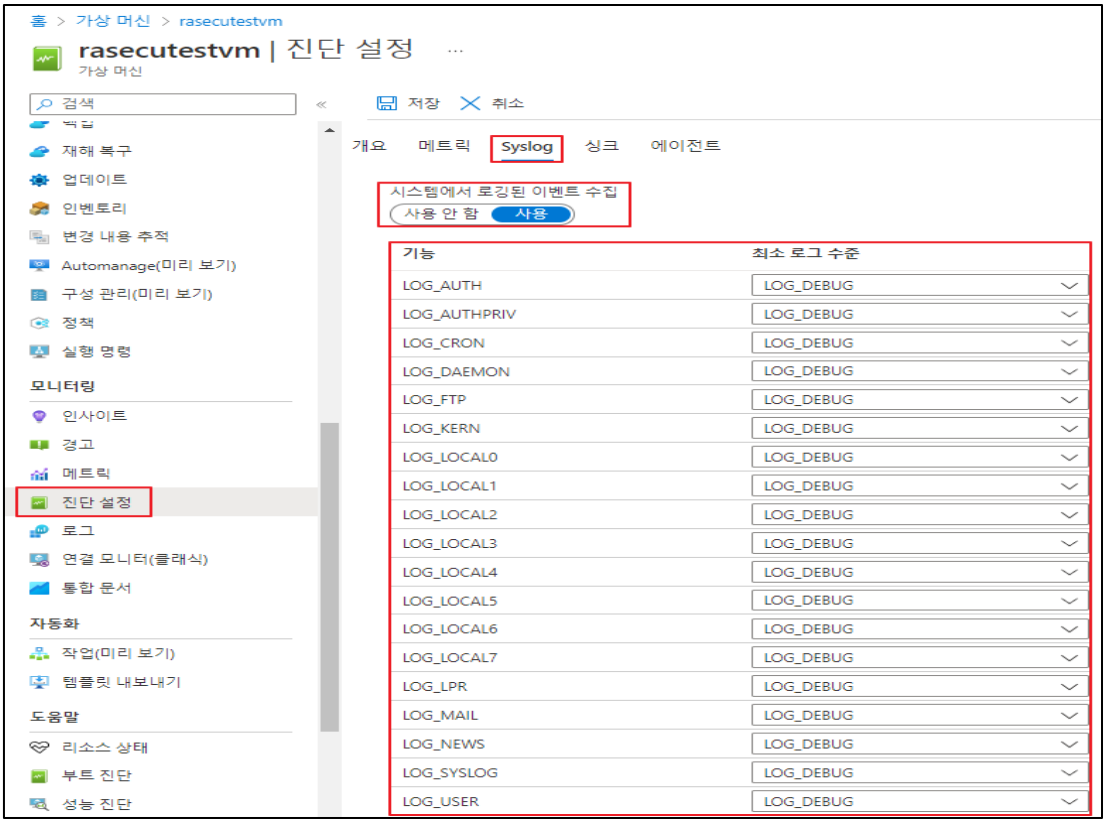
Syslog 는 Linux 에 공통적인 이벤트 로깅 프로토콜입니다. 애플리케이션은 로컬 시스템에 저장되거나 Syslog 수집기로 배달될 수 있는 메시지를 보냅니다. Linux 용 로그 분석 에이전트가 설치되면 에이전트에 메시지를 전달하도록 로컬 Syslog 디먼을 구성합니다. 그런 다음 에이전트는 해당 레코드가 만들어지는 Azure 모니터로 메시지를 보냅니다.

Linux 용 Log Analytics 에이전트는 구성에 지정된 기능 및 심각도가 있는 이벤트만 수집합니다. Azure 포털을 통해 또는 Linux 에이전트에서 구성 파일을 관리하여 시스템 로그를 구성할 수 있습니다.

※ 로그 전달 대상
<table>
<tr><th>구분</th><th>상세 내용</th></tr>
<tr><td>로그 분석 작업 영역</td><td>메트릭은 로그 형식으로 변환됩니다. 이 옵션은 모든 리소스 종류에 사용할 수 있는 것은 아닙니다. Azure Monitor 로그 저장소(Log Analytics를 통해 검색 가능)로 보내면 기존 로그 데이터를 사용하여 쿼리, 경고 및 시각화에 통합하는 데 도움이 됩니다.</td></tr>
<tr><td>Azure 저장소 계정</td><td>로그 및 메트릭을 Storage 계정에 보관하는 것은 감사, 정적 분석 또는 백업에 유용합니다. Azure Monitor 로그 또는 로그 분석 작업 영역을 사용하는 것과 비교할 때 저장소는 비용이 저렴하며 로그를 무기한 보관할 수 있습니다.</td></tr>
<tr><td>Azure Event Hubs</td><td>이벤트 허브에 로그 및 메트릭을 보낼 때 타사 SIEM 및 기타 Log Analytics 솔루션과 같은 외부 시스템으로 데이터를 스트리밍할 수 있습니다.</td></tr>
<tr><td>Azure 모니터 파트너 통합</td><td>Azure 모니터와 다른 타사 모니터링 플랫폼 간에 특수 통합을 수행할 수 있습니다. 통합은 파트너 중 하나를 이미 사용 중인 경우에 유용합니다.</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 인스턴스 서비스 감사 로그 스토리지 저장 설정 방법
1) 가상머신 메뉴 내 진단 설정 및 게스트 수준 모니터링 사용 버튼 선택</td></tr>
</table>



2) 가상머신 Syslog 이벤트 수집 활성화



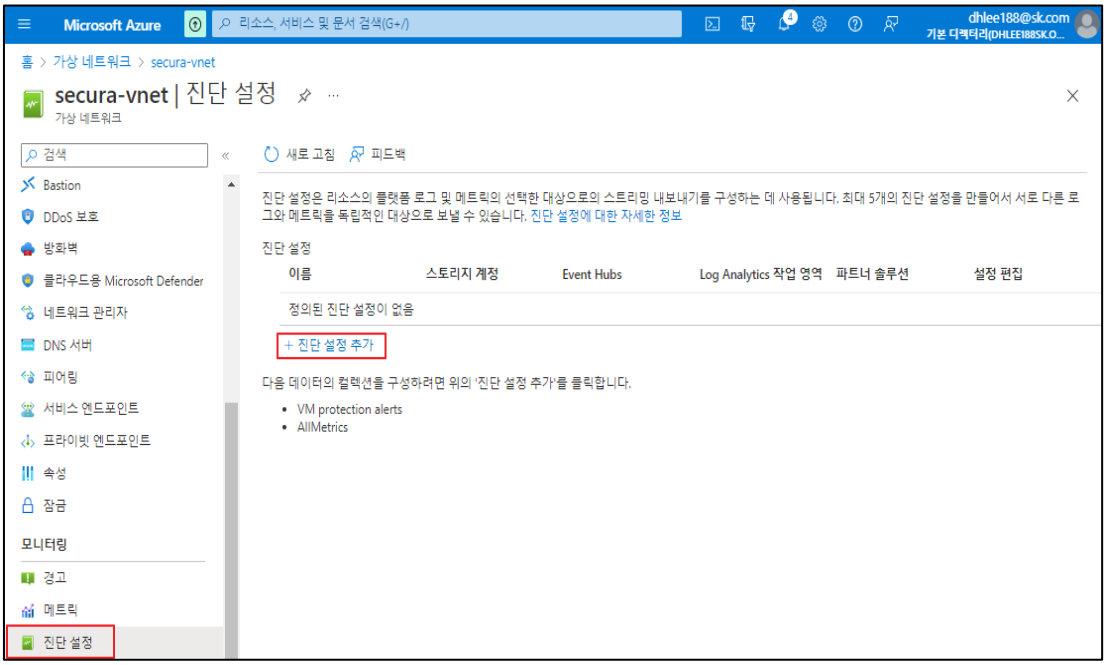
진단 기준	**양호기준** : 인스턴스 서비스 로그 보관 정책이 존재하고 있을 경우 **취약기준** : 인스턴스 서비스 로그 보관 정책이 존재하고 있지 않을 경우
비고	

4.8 네트워크 서비스 감사 로그 설정

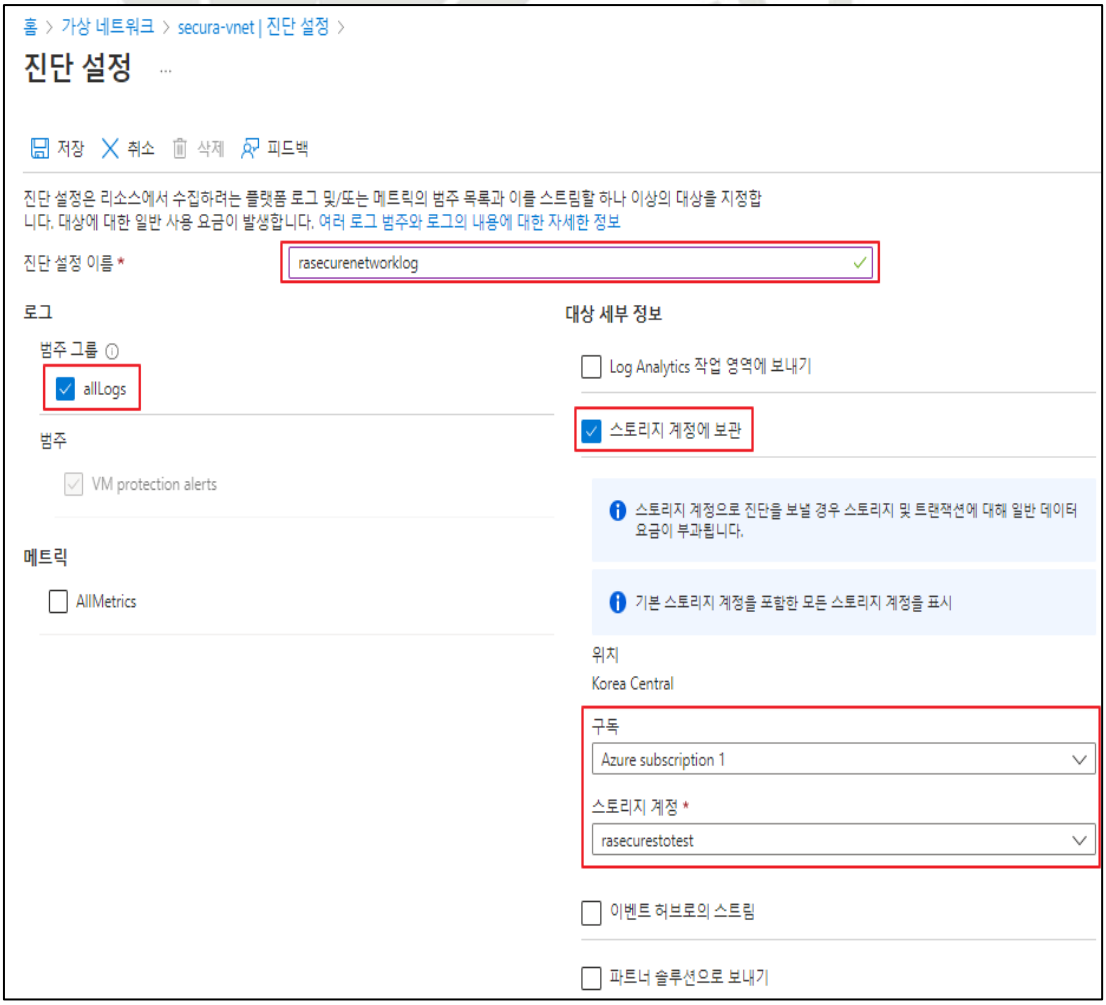
<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">네트워크 서비스 감사 로그 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure 가상 네트워크에서는 Azure Monitor 를 사용해 로그를 수집 분석 하며 플랫폼 메트릭 및 활동 로그는 자동으로 수집되고 저장되지만 진단 설정을 사용하여 다른 위치로 라우팅할 수 있습니다. 리소스 로그는 진단 설정을 만들고 하나 이상의 위치로 라우팅할 때까지 수집 및 저장되지 않습니다.

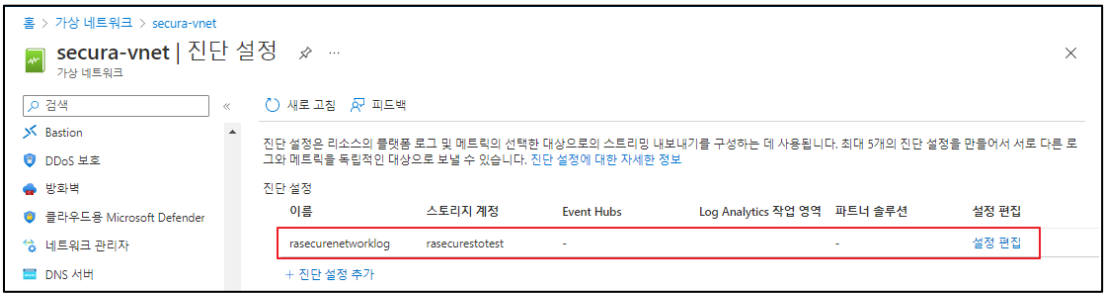
활동 로그는 구독 수준의 이벤트에 대한 인사이트를 제공하는 Azure 의 플랫폼 로그 유형입니다. 활동 로그는 독립적으로 보거나 Azure Monitor Logs 로 라우팅할 수 있습니다. 여기서 Log Analytics 를 사용하여 훨씬 더 복잡한 쿼리를 수행할 수 있습니다.

※ 로그 설정 구분
<table>
<tr><th>구분</th><th>상세내용</th></tr>
<tr><td>allLogs</td><td>리소스에서 제공하는 모든 리소스 로그입니다.</td></tr>
<tr><td>AllMetrics</td><td>상태 및 성능을 측정하는 Azure 서비스에서 내보내는 메트릭 데이터입니다.</td></tr>
</table>
※ 로그 전달 대상
<table>
<tr><th>구분</th><th>상세 내용</th></tr>
<tr><td>로그 분석 작업 영역</td><td>메트릭은 로그 형식으로 변환됩니다. 이 옵션은 모든 리소스 종류에 사용할 수 있는 것은 아닙니다. Azure Monitor 로그 저장소(Log Analytics를 통해 검색 가능)로 보내면 기존 로그 데이터를 사용하여 쿼리, 경고 및 시각화에 통합하는 데 도움이 됩니다.</td></tr>
<tr><td>Azure 저장소 계정</td><td>로그 및 메트릭을 Storage 계정에 보관하는 것은 감사, 정적 분석 또는 백업에 유용합니다. Azure Monitor 로그 또는 로그 분석 작업 영역을 사용하는 것과 비교할 때 저장소는 비용이 저렴하며 로그를 무기한 보관할 수 있습니다.</td></tr>
<tr><td>Azure Event Hubs</td><td>이벤트 허브에 로그 및 메트릭을 보낼 때 타사 SIEM 및 기타 Log Analytics 솔루션과 같은 외부 시스템으로 데이터를 스트리밍할 수 있습니다.</td></tr>
<tr><td>Azure 모니터 파트너 통합</td><td>Azure 모니터와 다른 타사 모니터링 플랫폼 간에 특수 통합을 수행할 수 있습니다. 통합은 파트너 중 하나를 이미 사용 중인 경우에 유용합니다.</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 네트워크 서비스 감사 로그 스토리지 저장 설정 방법
1) 가상 네트워크 메뉴 내 진단 설정 추가 버튼 선택</td></tr>
</table>



2) 네트워크 로그 수집 활성화 및 스토리지 계정 선택 후 저장



	3) 진단 설정 목록 내 정상 생성 유무 확인 
진단 기준	**양호기준** : 네트워크 서비스 로그 보관 정책이 존재하고 있을 경우 **취약기준** : 네트워크 서비스 로그 보관 정책이 존재하고 있지 않을 경우
비고	

4.9 기타 서비스 감사 로그 설정

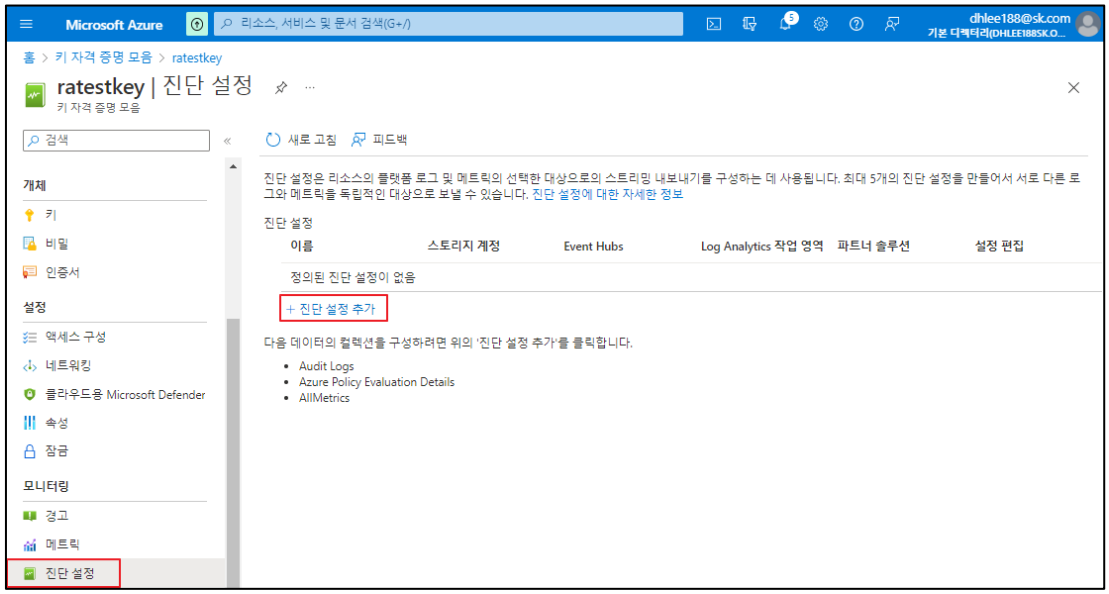
<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">기타 서비스 감사 로그 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure 리소스 내 기타 서비스의 경우 Azure Monitor 내 진단 설정을 통해 로그를 기록 / 정의 할 수 있습니다. 크게 플랫폼 로그 / 리소스 로그 / 활동 로그로 구분 됩니다.

플랫폼 로그에서 Azure 리소스 및 이에 따른 Azure 플랫폼에 관한 자세한 진단 및 감사 정보를 제공합니다. 자동으로 생성되지만 특정 플랫폼 로그를 하나 이상의 대상으로 전달하여 보존하도록 구성해야 합니다.

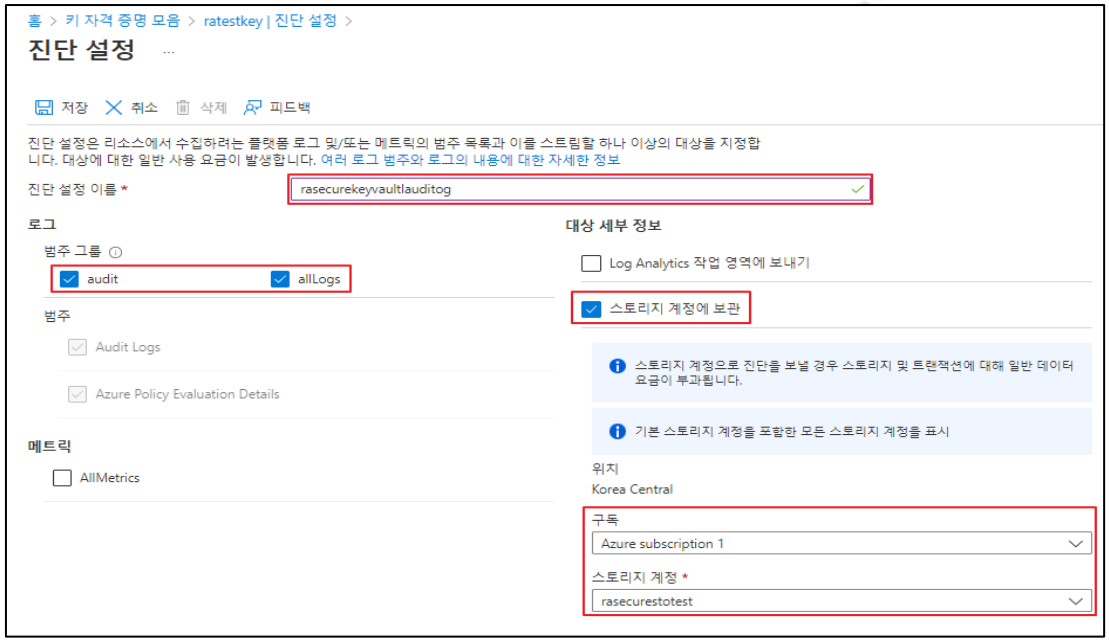
Azure 리소스 로그는 Azure 리소스 내에서 수행된 작업에 대한 인사이트를 제공하는 플랫폼 로그입니다. 이러한 로그의 내용은 Azure 서비스와 리소스 종류에 따라 달라집니다. 리소스 로그는 기본적으로 수집되지 않습니다.

마지막으로 활동 로그는 구독 수준 이벤트에 대한 정보를 제공하는 Azure 의 플랫폼 로그입니다. 활동 로그에는 리소스가 수정되거나 가상 머신이 시작될 때와 같은 정보가 포함됩니다.

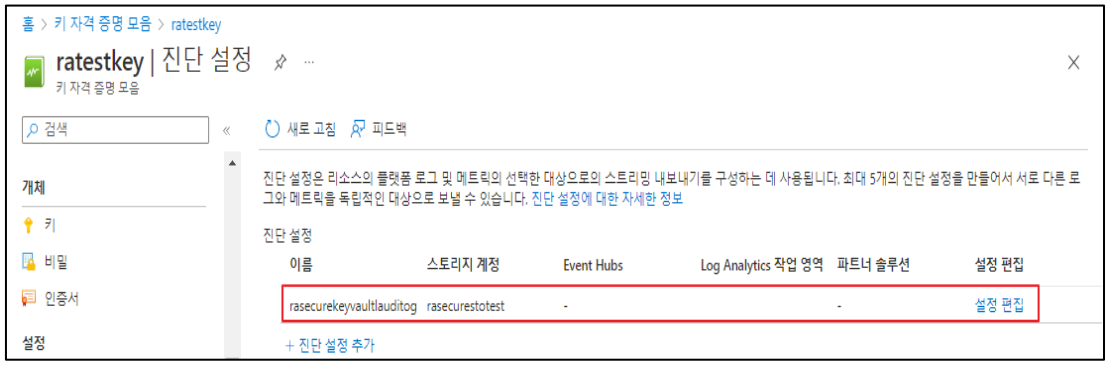
※ 로그 전달 대상
<table>
<tr><th>구분</th><th>상세 내용</th></tr>
<tr><td>로그 분석 작업 영역</td><td>메트릭은 로그 형식으로 변환됩니다. 이 옵션은 모든 리소스 종류에 사용할 수 있는 것은 아닙니다. Azure Monitor 로그 저장소(Log Analytics를 통해 검색 가능)로 보내면 기존 로그 데이터를 사용하여 쿼리, 경고 및 시각화에 통합하는 데 도움이 됩니다.</td></tr>
<tr><td>Azure 저장소 계정</td><td>로그 및 메트릭을 Storage 계정에 보관하는 것은 감사, 정적 분석 또는 백업에 유용합니다. Azure Monitor 로그 또는 로그 분석 작업 영역을 사용하는 것과 비교할 때 저장소는 비용이 저렴하며 로그를 무기한 보관할 수 있습니다.</td></tr>
<tr><td>Azure Event Hubs</td><td>이벤트 허브에 로그 및 메트릭을 보낼 때 타사 SIEM 및 기타 Log Analytics 솔루션과 같은 외부 시스템으로 데이터를 스트리밍할 수 있습니다.</td></tr>
<tr><td>Azure 모니터 파트너 통합</td><td>Azure 모니터와 다른 타사 모니터링 플랫폼 간에 특수 통합을 수행할 수 있습니다. 통합은 파트너 중 하나를 이미 사용 중인 경우에 유용합니다.</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 기타 서비스 감사 로그 스토리지 저장 설정 방법
1) 키 자격 증명 모음 메뉴 내 진단 설정 추가 버튼 선택</td></tr>
</table>



2) 키 자격 증명 모음 로그 수집 활성화 및 스토리지 계정 선택 후 저장

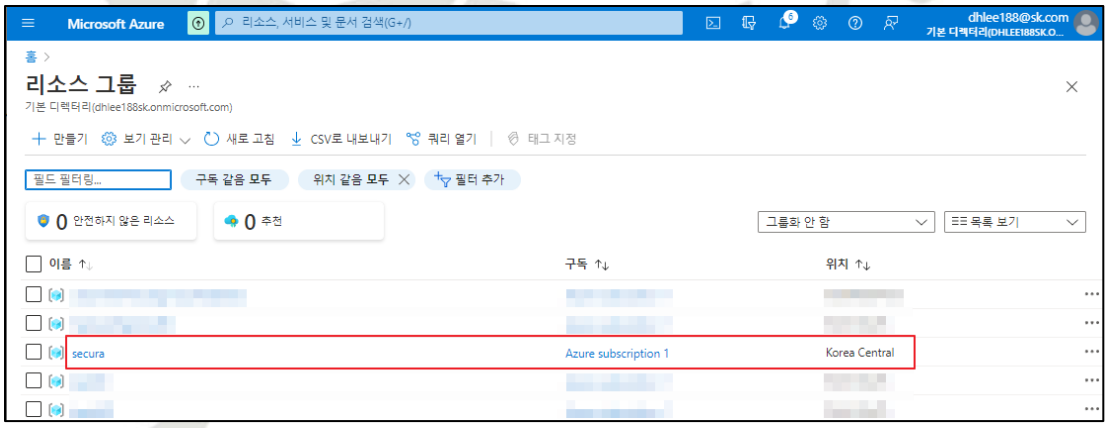
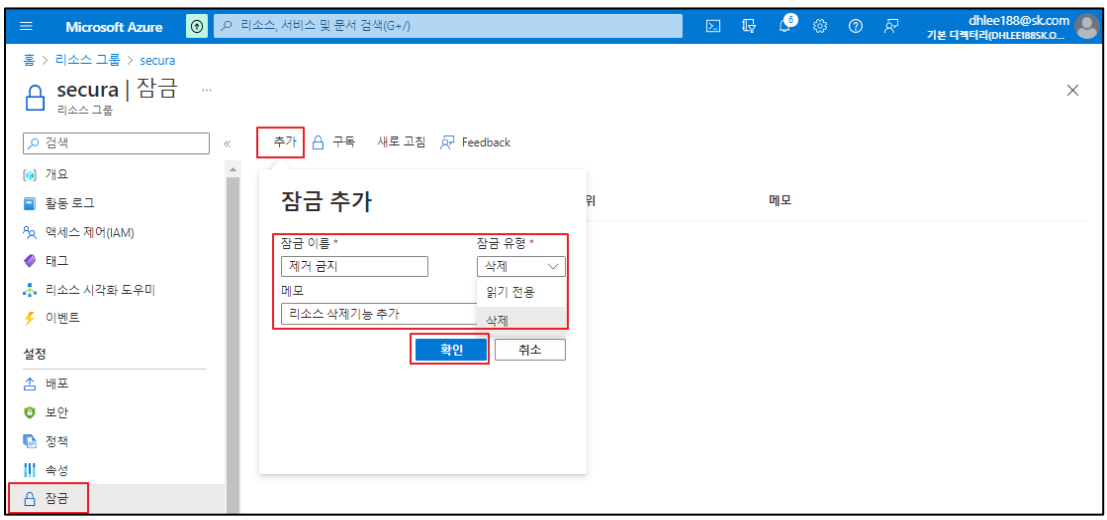


3) 진단 설정 목록 내 정상 생성 유무 확인



진단 기준	**양호기준** : 기타 서비스 로그 보관 정책이 존재하고 있을 경우 **취약기준** : 기타 서비스 로그 보관 정책이 존재하고 있지 않을 경우
비고	

4.10 리소스 그룹 잠금

분류	운영 관리	중요도	하
항목명	리소스 그룹 잠금		
항목 설명	관리자는 구독, 리소스 그룹 또는 리소스에 잠금을 설정하여 조직의 다른 사용자가 실수로 중요한 리소스를 삭제 또는 수정하지 못하게 할 수 있습니다. 잠금 수준을 CanNotDelete 또는 ReadOnly 로 설정할 수 있습니다. 포털에서 잠금은 각각 삭제 및 읽기 전용으로 지칭됩니다. 삭제 및 읽기전용 중 하나라도 설정할 경우 리소스는 삭제되지 않으며, 리소스 그룹 잠금을 설정하지 않을 경우 리소스를 '읽기','수정', '삭제' 할 수 있음 **※ 리소스 그룹 잠금 수준** - CanNotDelete(삭제): 권한이 부여된 사용자가 읽기/수정은 가능하지만 삭제는 불가 - ReadOnly(읽기전용): 권한이 부여된 사용자가 읽기만 가능		
설정 방법	**가. 리소스 그룹 잠금 설정 방법** 1) 리소스 그룹 선택  2) 리소스 그룹 잠금 설정  		

	3) 생성된 잠금 설정 확인 
진단 기준	**양호기준** : 고객서비스(상용) 및 운영서비스가 잠금 기능을 설정하여 사용하고 있을 경우 **취약기준** : 고객서비스(상용) 및 운영서비스가 잠금 기능을 설정하여 사용하고 있지 않을 경우
비고	

4.11 백업 사용 여부

분류	운영 관리	중요도	중
항목명	백업 사용 여부		
항목 설명	운영중인 클라우드 리소스에 대한 시스템 충돌, 장애 발생, 인적 재해 등 기업의 사업 연속성을 해치는 모든 상황에 대비하기 위해 백업 서비스를 구성해야 데이터를 안전하게 보관할 수 있습니다. 이에 보안담당자 및 관리자는 클라우드 리소스에 대한 백업을 설정하여 데이터 손실을 방지 할 수 있도록 정책을 수립하고 관리하여야 합니다.		
설정 방법	**가. 백업 및 복구 절차 수립** 1) 백업 및 복구 절차 수립, 담당자 지정 - 백업대상(서버 이미지, DB 데이터, 보안로그 등) 선정 - 백업대상별 백업 주기 및 보존기한 정의 - 백업 담당자 및 책임자 지정 - 백업방법 및 절차: 백업시스템 활용, 매뉴얼 방식 등(백업매체 관리 포함) - 복구절차 - 백업이력관리 (백업 관리 대장) - 백업 소산에 대한 물리적·지역적 사항 고려 - 백업 사이트 구축 및 운영 **※ 클라우드서비스 보안인증제도(IaaS) 평가기준 해설서의 "6.2 서비스 가용성" 항목 참고**		
진단 기준	**양호기준** : 클라우드 리소스 백업 정책이 존재하는 경우 **취약기준** : 클라우드 리소스 백업 정책이 존재하지 않는 경우		
비고			

2023 클라우드 보안 가이드
- Azure

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 취약점진단팀
제　작 : SK쉴더스 커뮤니케이션그룹