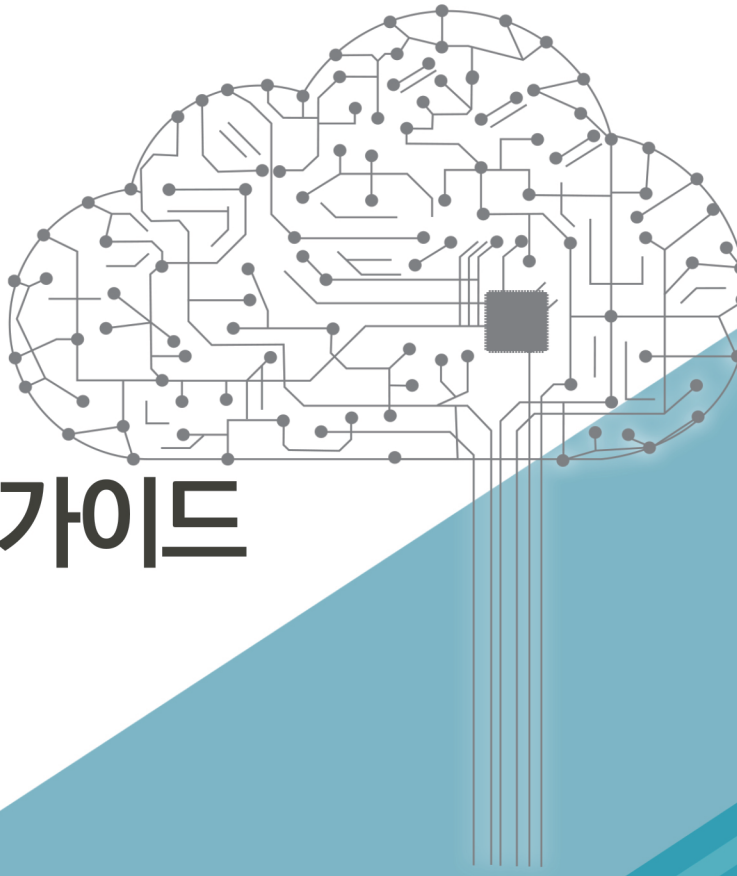
ADT캡스 | infosec



2021 클라우드 보안 가이드

-Azure

클라우드 보안 가이드 2021 발간사

안녕하십니까? ADT캡스 인포섹입니다.
지난 2019년 인포섹의 취약점진단팀은 '클라우드 보안 가이드 - AWS, Cloud Z', '클라우드 보안 가이드(컨테이너 보안) - Docker, Kubernetes', '클라우드 보안 가이드 - Azure, GCP'를 발간했습니다.

그동안 AWS, Azure, GCP는 빠르게 변화했으며, 이러한 트렌드를 분석하고 변화에 대응하고자 올해 '클라우드 보안 가이드 - AWS, Azure, GCP' 3종의 개정판을 발간하게 되었습니다.

매년 클라우드 환경으로 전환하는 기업들이 늘어나고 있으며, 클라우드 도입 및 전환 시 미흡한 환경설정 및 보안정책 설정으로 인한 해킹공격이 발생하고 있습니다.

이번 가이드는 계정 관리, 권한 관리, 데이터 관리, 가상 리소스 관리, 감사/추적 관리 영역으로 분류됐으며, 각 영역별 보안 정책 설정 방법과 점검 방법에 대한 설명을 담고 있습니다. 또한, 취약점 점검 항목을 포함하여 클라우드 운영자가 위협에 대응하고 인증 심사와 컴플라이언스 기준을 충족할 수 있는 기준을 제시했습니다.

앞으로도 ADT캡스 인포섹은 클라우드 운영자가 다양한 환경에 발빠르게 대응할 수 있도록 보안 가이드를 발간할 계획입니다.

더불어, 1년 동안 클라우드 보안 가이드 개선에 많은 시간과 노력을 투자한 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 자료 문서(Microsoft docs : https://docs.microsoft.com/ko-kr/azure/) 및 국내 발간 서적(마스터링 Microsoft Azure IaaS 등) 자료를 바탕으로 작성하였으며, 각각 권한관리(7개 항목), 계정관리(8개 항목), 데이터관리(4개 항목), 가상 리소스 관리(14개 항목), 감사추적(2개 항목)으로 총 5개 영역에서 35개 항목으로 구성되어 있습니다.

[표] 1. Microsoft Azure 보안진단 체크리스트

영역	항목코드	항목명	중요도
권한관리	1.1	불필요한 리소스 그룹 정책 관리	중
	1.2	리소스 그룹 잠금	중
	1.3	액세스 제어(IAM) 최고 권한 역할 할당	상
	1.4	액세스 제어(IAM) 역할 할당	상
	1.5	AD 관리자 역할 할당	상
	1.6	AD 일반 계정 역할 할당	중
	1.7	Key Vault 액세스 정책 관리	상
계정관리	2.1	AD 사용자 계정 최고 권한 관리	상
	2.2	AD User 프로필 및 디렉터리 식별 관리	중
	2.3	AD 그룹 구성원 및 소유자 관리	중
	2.4	AD 게스트 사용자	상
	2.5	AD 암호 재설정 관리	하
	2.6	MFA (Multi-Factor Authentication) 설정	상
	2.7	MFA 잠금 정책 관리	중
	2.8	Azure 패스워드 정책 관리	중
데이터관리	3.1	투명한 데이터 암호화 (TDE)	중
	3.2	애플리케이션 게이트웨이 암호화	상
	3.3	애플리케이션 게이트웨이 풀 관리	중
	3.4	Key Vault 암호화 설정	상
가상 리소스 관리	4.1	가상 네트워크 디바이스 설정	상
	4.2	서브넷	하
	4.3	내부 가상 네트워크 보안 관리	상
	4.4	가상 네트워크 게이트웨이 연결 관리	상
	4.5	보안그룹 인/아웃바운드 ANY 설정 관리	상
	4.6	보안그룹 인/아웃바운드 불필요 정책 관리	상
	4.7	방화벽 인/아웃바운드 ANY 설정 관리	상
	4.8	방화벽 인/아웃바운드 불필요 정책 관리	중
	4.9	가상 Compute 안전한 SSH 연결	중
	4.10	SSH Key 관리	하

	4.11	스토리지 계정 보안 설정	상
	4.12	스토리지 계정 권한 관리	상
	4.13	스토리지 계정 공유 액세스 서명 사용 관리	상
	4.14	스토리지 계정 공유 액세스 서명 정책 관리	중
감사추적	5.1	AD 감사 로그	하
	5.2	Azure 모니터 로그 통합 (Log Analytics)	하

2. 위험도 구분

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

[표] 2. 위험도 구분

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

II. 세부항목 설정

1. 권한관리

1.1 불필요한 리소스 그룹 정책 관리

<table>
<tr><td>분류</td><td>권한관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">불필요한 리소스 그룹 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure 솔루션에 관련된 리소스를 보유하는 컨테이너로서 리소스 그룹은 그룹으로 관리하려는 리소스만 포함합니다. 이에 조직에 가장 적합한 내용에 따라 리소스 그룹에 리소스를 어떻게 할당할지 결정합니다. 리소스 그룹은 Azure 리소스 매니저를 통해 관리되며 '데이터저장소', 'Web App', 'Virtual Machine'등과 같은 각각의 리소스를 그룹화하여 관리할 수 있습니다.

※ IAM 사용자 역할
<table>
<tr><th>역할 이름
(한글)</th><th>역할 이름
(영문)</th><th>상세설명</th></tr>
<tr><td>소유자</td><td>Owner</td><td>리소스 액세스를 비롯한 모든 것을 관리함</td></tr>
<tr><td>기여자</td><td>Contributor</td><td>리소스 액세스를 제외한 모든 것을 관리함</td></tr>
<tr><td>독자</td><td>Reader</td><td>모든 항목을 볼 수 있지만 변경할 수 있는 권한은 없음</td></tr>
<tr><td>Avere 연산자</td><td>Avere Contributor</td><td>Avere vFXT 클러스터에서 클러스터를 관리함</td></tr>
<tr><td>Avere 참가자</td><td>Avere Operator</td><td>Avere vFXT 클러스터를 만들고 관리함</td></tr>
<tr><td>DevTest Labs 사용자</td><td>DevTest Labs User</td><td>Azure DevTest Labs 의 가상 머신 연결, 시작, 다시 시작 및 종료할 수 있음</td></tr>
<tr><td>Log Analytics 독자</td><td>Log Analytics Reader</td><td>Log Analytics 독자는 모든 Azure 리소스에 대한 Azure Diagnostics 의 구성 보기를 비롯하여 모니터링 설정 보기 및 모든 모니터링 데이터를 보고 검색할 수 있음</td></tr>
<tr><td>Log Analytics 참가자</td><td>Log Analytics Contributor</td><td>Log Analytics 참가자는 모든 모니터링 데이터를 읽고 모니터링 설정을 편집할 수 있습니다. 모니터링 설정 편집에는 VM 에 VM 확장 추가,
Azure Storage 에서 로그 컬렉션을 구성할 수 있는 스토리지 계정 키 읽기, Automation 계정 생성 및 구성, 솔루션 추가 및
모든 Azure 리소스에 대한 Azure Diagnostics 을 구성하는 기능도 포함되어 있습니다.</td></tr>
<tr><td>Logic Apps 참가자</td><td>Logic App Contributor</td><td>Logic Apps 을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음</td></tr>
<tr><td>Site Recovery 운영자</td><td>Site Recovery Operator</td><td>장애 조치(failover) 및 장애 복구(failback)를 수행할 수 있지만 다른 Site Recovery 관리 작업은 수행할</td></tr>
</table>
</td></tr>
</table>

		수 없음
Site Recovery 참가자	Site Recovery Contributor	자격 증명 모음 만들기 및 역할 할당을 제외한 Site Recovery 서비스를 관리할 수 있음
Storage Blob 데이터 Contributor	Storage Blob Data Contributor	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage Blob 데이터 Reader	Storage Blob Data Reader	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기 액세스를 허용
Storage Blob 데이터 소유자	Storage Blob Data Owner	POSIX 액세스 제어 할당을 포함하여 Azure Storage Blob 컨테이너 및 데이터에 대한 모든 권한 허용
Storage 계정 참가자	Storage Account Contributor	Storage 계정을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음
Storage 큐 데이터 Contributor	Storage Queue Data Contributor	Azure Storage 큐 및 큐 메시지에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage 큐 데이터 Reader	Storage Queue Data Reader	Azure Storage 큐 및 큐 메시지에 대한 읽기 액세스를 허용
Storage 큐 데이터 메시지 보낸 사람	Storage Queue Data Message Sender	Azure Storage 큐 메시지 보내기 허용
Storage 큐 데이터 메시지 프로세서	Storage Queue Data Message Processor	Azure Storage 큐 메시지에 대한 미리 보기, 수신 및 삭제 권한 허용
가상 머신 참가자	Virtual Machine Contributor	가상 컴퓨터를 관리할 수 있지만 가상 컴퓨터나 가상 컴퓨터가 연결된 가상 네트워크 또는 저장소 계정에 액세스 할 수 없음
관리되는 애플리케이션 운영자 역할	Managed Application Operator Role	관리되는 애플리케이션 리소스에서 작업을 읽고 수행할 수 있음
관리되는 애플리케이션 판독기	Managed Application Reader	관리되는 앱에서 리소스를 읽고 JIT 액세스 권한을 요청할 수 있음
리소스 정책 참가자(미리 보기)	Resource Policy Contributor (Preview)	(미리 보기) 리소스 정책을 생성/수정하고, 지원 티켓을 만들고, 리소스/계층 구조를 읽을 수 있는 권한을 가진 EA 의 백필된 사용자
모니터링 리더	Monitoring Reader	모든 모니터링 데이터를 읽을 수 있음
모니터링 메트릭 게시자	Monitoring Metrics Publisher	Azure 리소스에 대해 메트릭을 게시할 수 있음

모니터링 참가자	Monitoring Contributor	모든 모니터링 데이터를 읽고 모니터링 설정을 업데이트할 수 있음
백업 운영자	Backup Operator	백업 제거를 제외한 백업 서비스를 관리하고 자격 증명 모음 만들고 다른 사람에게 액세스 권한을 부여할 수 있음
백업 참가자	Backup Contributor	백업 서비스를 관리할 수 있지만, 자격 증명 모음을 만들고 다른 사용자에게 액세스 권한을 부여할 수 없음
사용자 액세스 관리자	User Access Administrator	Azure 리소스에 대한 사용자 액세스를 관리할 수 있음
스토리지 계정 키 운영자 서비스 역할	Storage Account Key Operator Service Role	스토리지 계정 키 운영자가 스토리지 계정에서 키를 나열하고 다시 생성할 수 있음
읽기 권한자 및 데이터 액세스	Reader and Data Access	모든 항목을 볼 수 있지만, 스토리지 계정 또는 포함된 리소스를 삭제하거나 만들 수는 없고, 스토리지 계정 키에 액세스하면 스토리지 계정에 포함된 모든 데이터에 대한 읽기/쓰기 액세스가 허용됩니다.

※ IAM 역할별 권한 관리 (예시)

역할	IAM 관리형 정책명
Console 관리자	Owner(소유자)
Infra 관리자	Contridutor(기여자), Site Recovery Contributor(Site Recovery 참가자), Backup Operator(백업 운영자), User Access Administrator(사용자 액세스 관리자)
Infra 운영 및 담당자	Reader(독자), DevTest Labs User(DevTest Labs 사용자), Virtual Machine Contributor(가상 머신 참가자), Site Recovery Operator(Site Recovery 운영자), Backup Contributor(백업 참가자)
Application 관리자	Managed Application Operator Role(관리되는 애플리케이션 운영자 역할)
Application 운영 및 담당자	Logic App Contributor(Logic Apps 참가자), Managed Application Reader(관리되는 애플리케이션 판독기)
개발 관리자	Storage Blob Data Owner(Storage Blob 데이터 소유자), Storage Queue Data Contributor(Storage 큐 데이터 Contributor)
개발 운영 및 담당자	Storage Blob Data Contributor(Storage Blob 데이터 Contributor), Storage Blob Data Reader(Storage Blob 데이터 Reader), Storage Account Contributor(Storage 계정 참가자), Storage Queue Data Message Processor(Storage 큐 데이터 메시지 프로세서), Storage Queue Data Message Sender(Storage 큐 데이터

	메시지 보낸 사람), Storage Queue Data Reader(Storage 큐 데이터 Reader), Storage Account Key Operator Service Role(스토리지 계정 키 운영자 서비스 역할)
보안 관리자	Log Analytics Contributor(Log Analytics 참가자), Resource Policy Contributor (리소스 정책 참가자(미리 보기)), User Access Administrator(사용자 액세스 관리자)
보안 운영 및 담당자	Log Analytics Reader(Log Analytics 독자), Storage Account Key Operator Service Role(스토리지 계정 키 운영자 서비스 역할)
로깅 관리자	Monitoring Contributor(모니터링 참가자)
로깅 운영 및 담당자	Monitoring Reader(모니터링 리더), Monitoring Metrics Publisher(모니터링 메트릭 게시자)
재무/비용 관리자	Reader and Data Access(읽기 권한자 및 데이터 액세스)

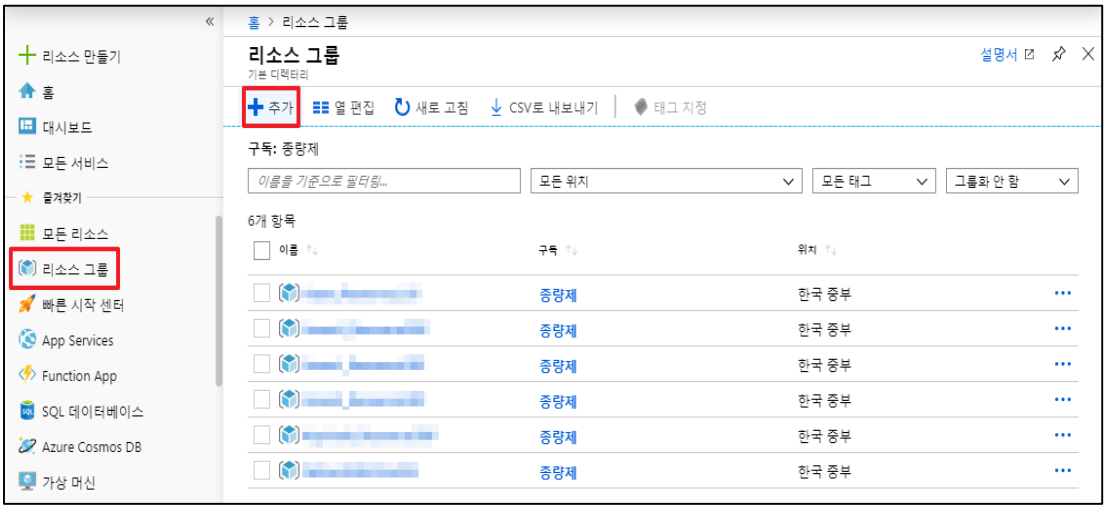
※ IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	관리형 정책	취약 유/무
Console 관리자	Ex)Owner(소유자)	Ex)Owner(소유자)	N/A
Infra 관리자/운영 및 담당자			N/A
Application 관리자/ 운영 및 담당자			N/A
개발 관리자/ 운영 및 담당자			N/A
재무 / 비용 관리자 및 담당자			N/A

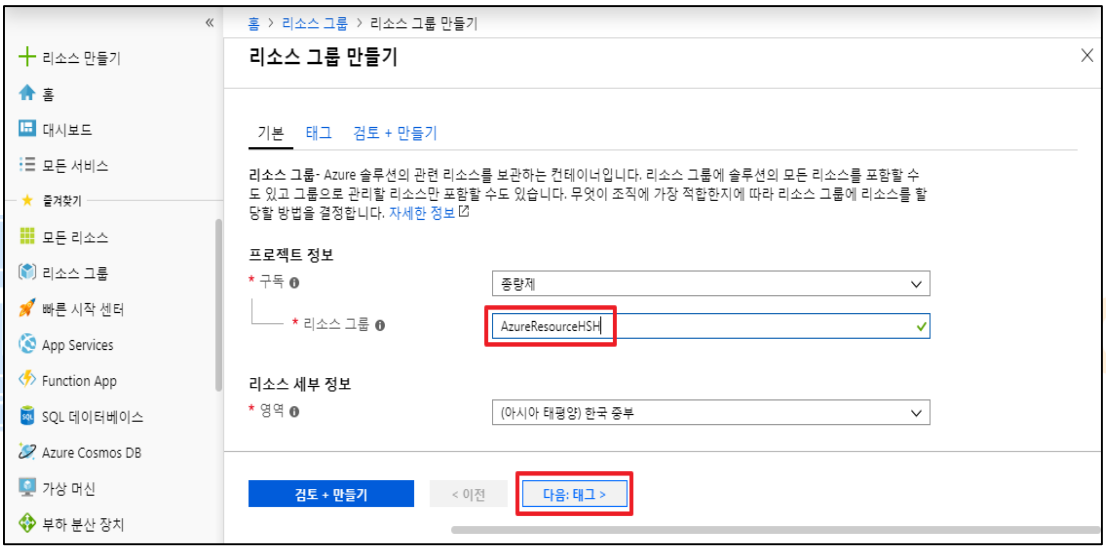
설정 방법

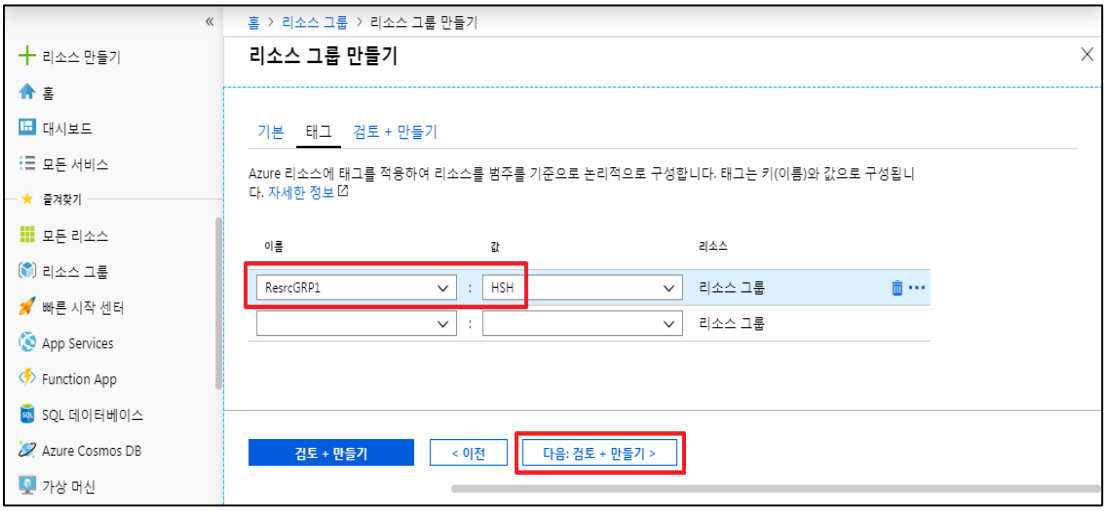
가. 리소스 그룹 생성 방법

1) 리소스 그룹 메뉴 내 추가 버튼 클릭

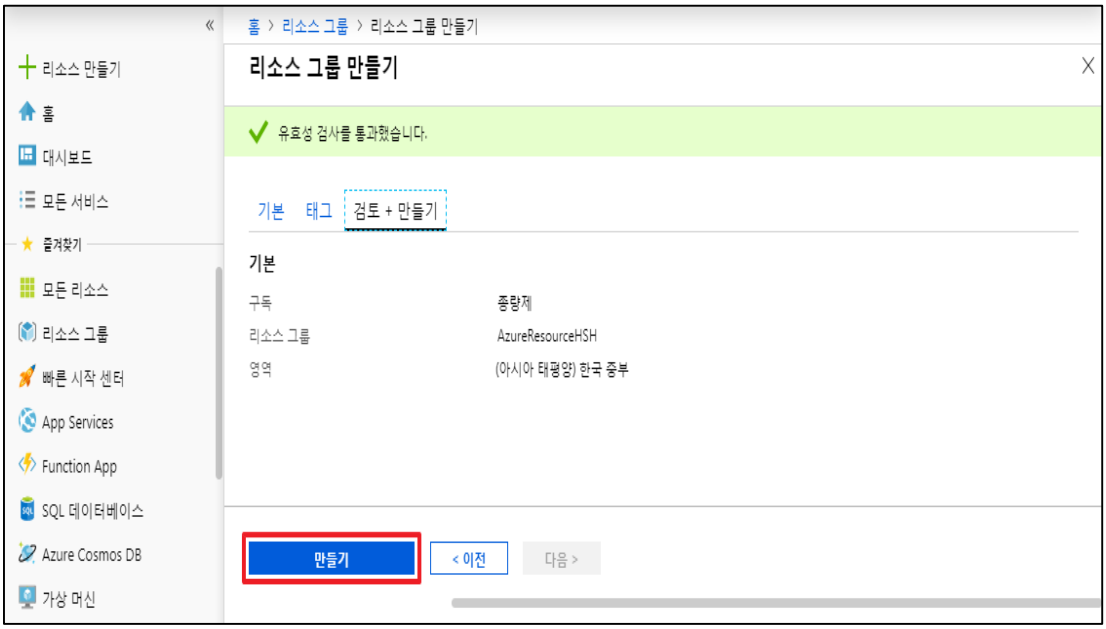


2) 리소스 그룹명 및 태그 설정

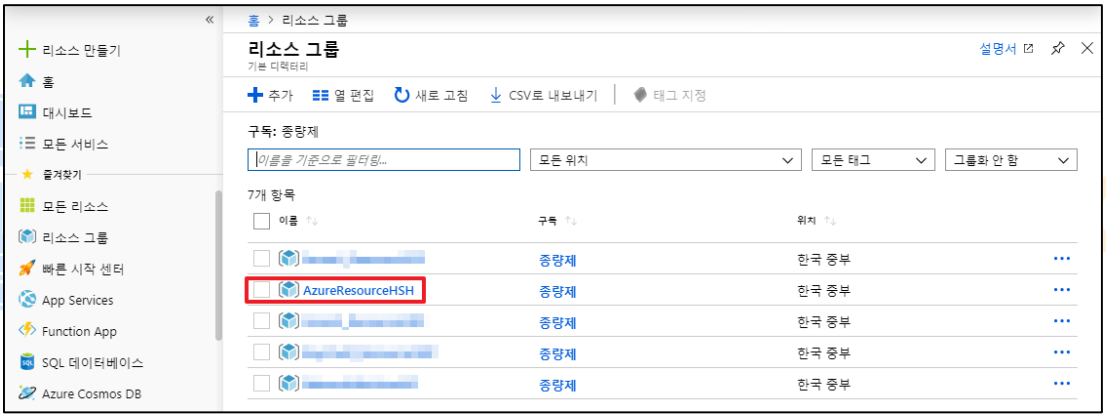




3) 리소스 그룹 검토 및 만들기

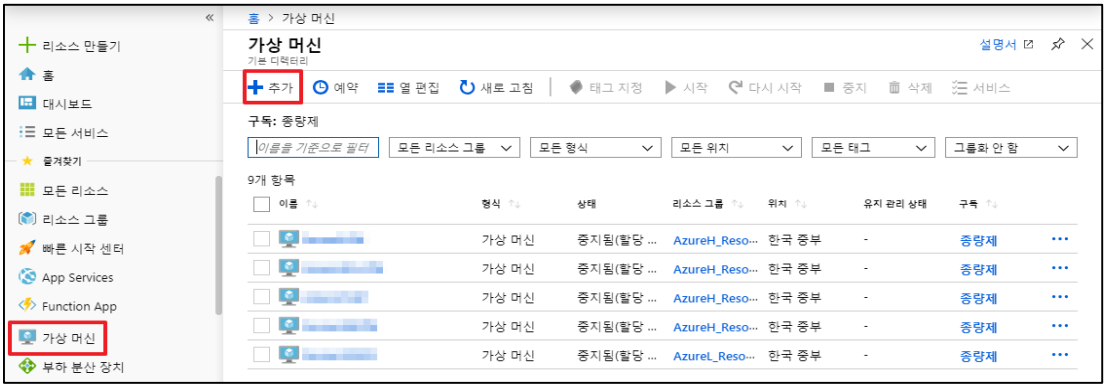


4) 생성된 리소스 그룹 확인



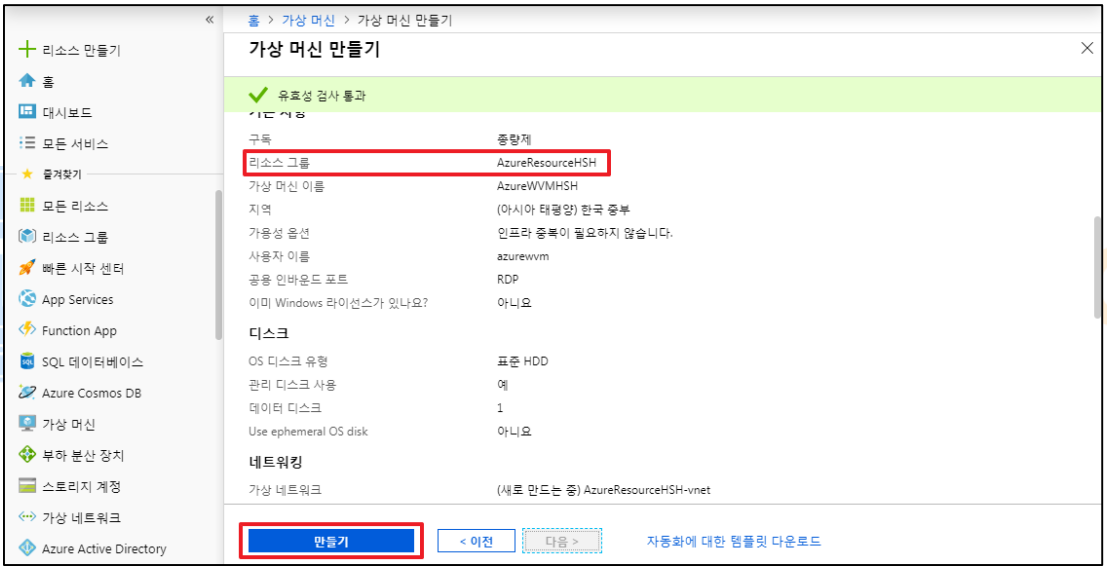
나. 리소스 그룹 내 리소스 생성 및 할당 방법 (예: 가상머신 추가)

1) 가상머신 메뉴 내 추가 버튼 클릭

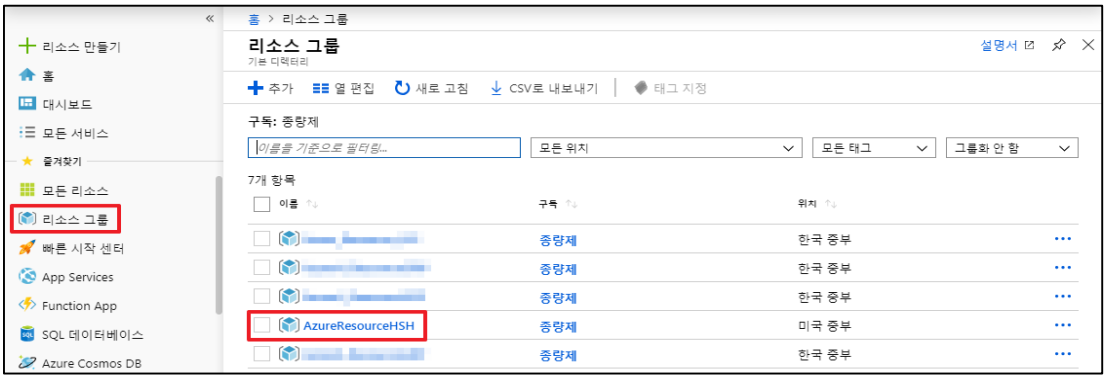


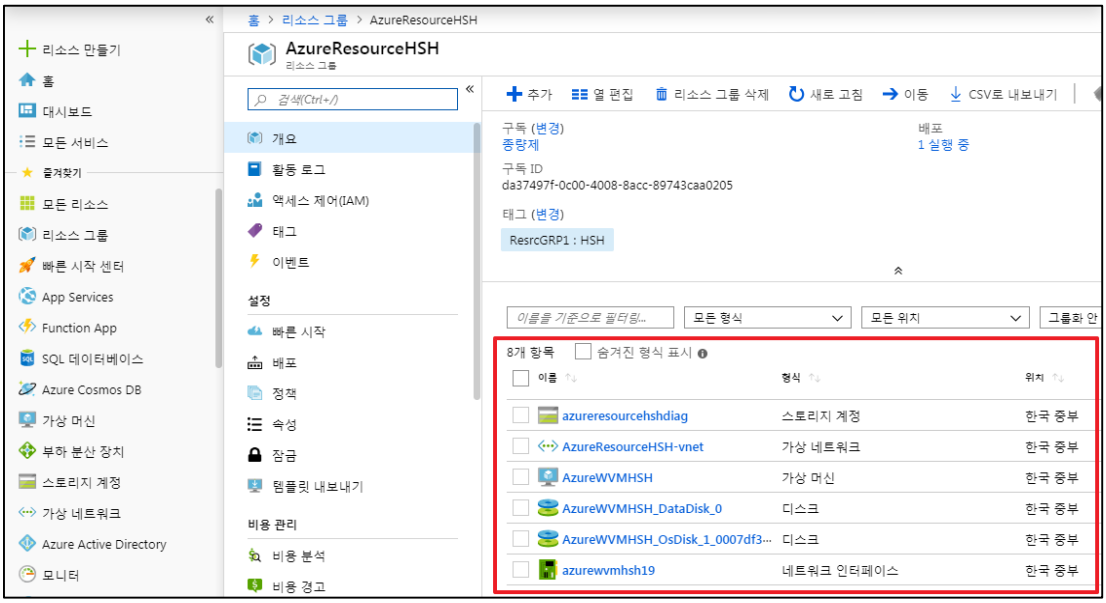
2) 리소스 그룹 선택 및 리소스(가상머신) 옵션 설정

3) 설정된 리소스(가상머신) 검토 및 만들기



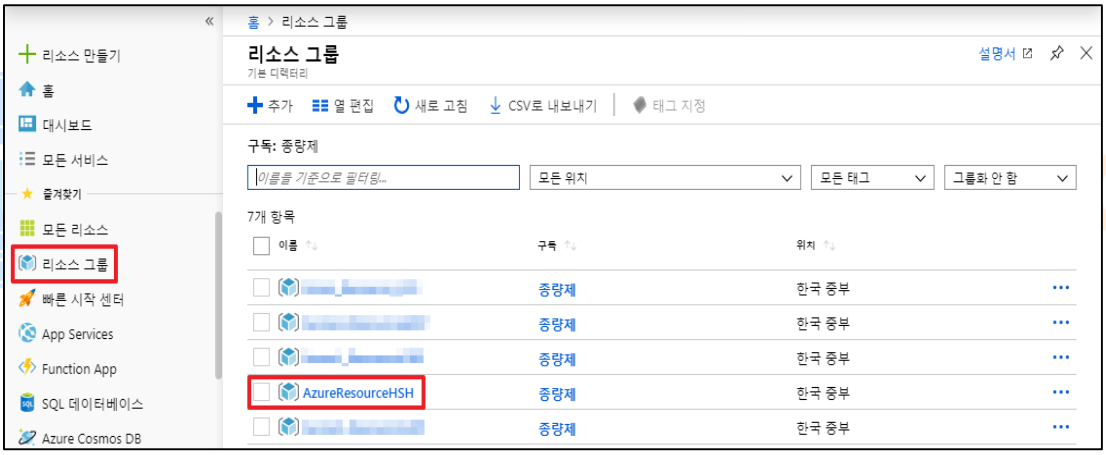
4) 리소스 그룹 메뉴 선택 및 생성 및 할당된 리소스(가상머신) 정상 생성 유무 확인



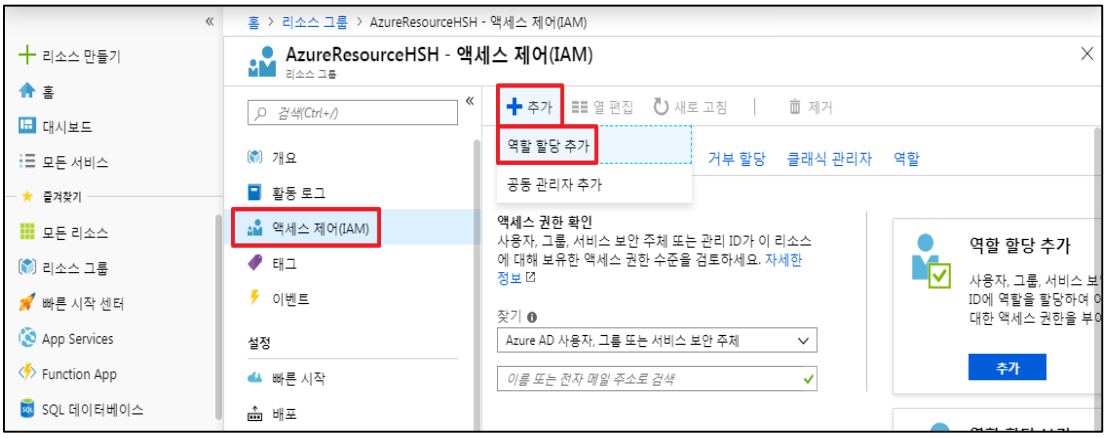


다. 리소스 그룹 내 액세스 제어(IAM) 설정 방법

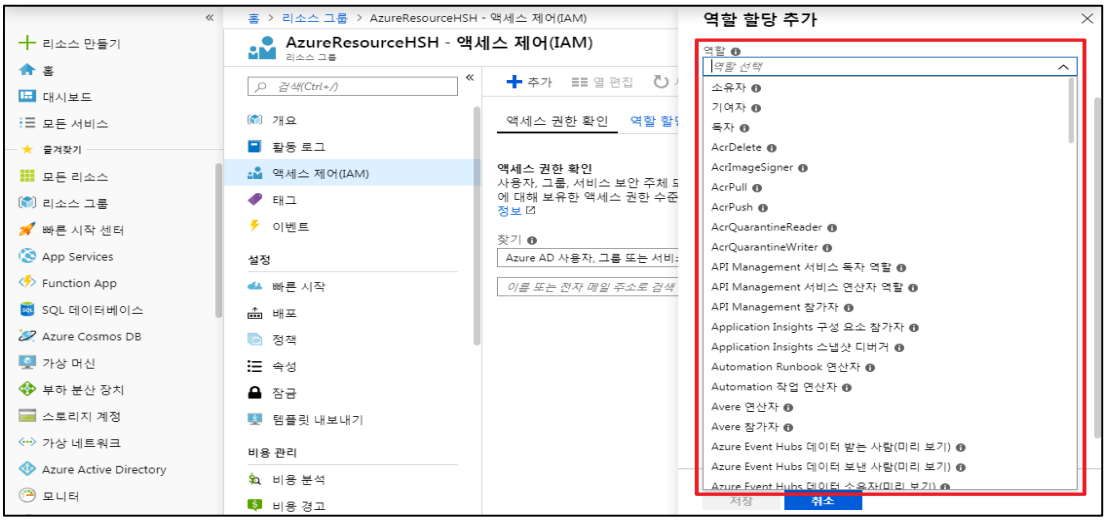
1) 액세스 제어를 설정할 리소스 그룹 선택



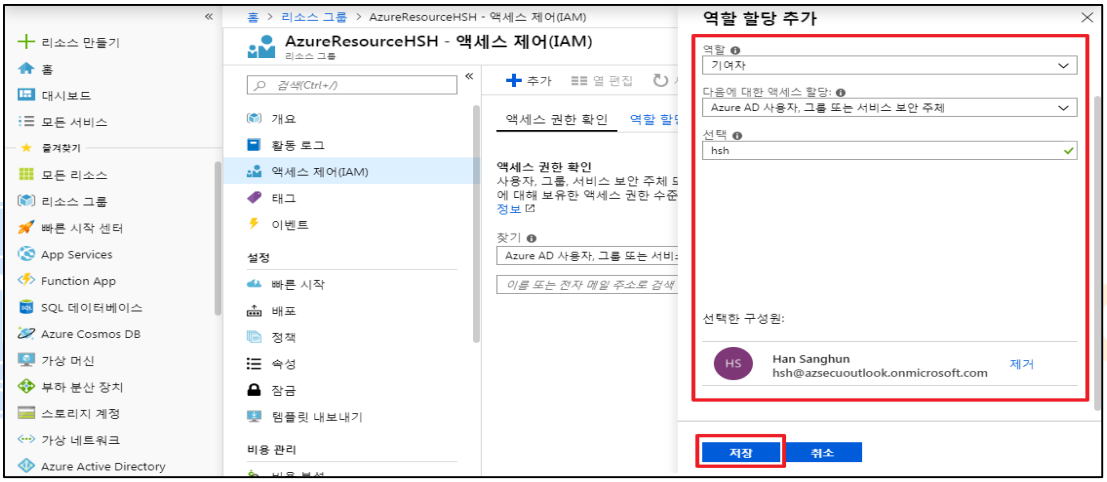
2) 리소스 그룹 내 액세스 제어(IAM) 선택 후 역할 할당 추가 버튼 클릭



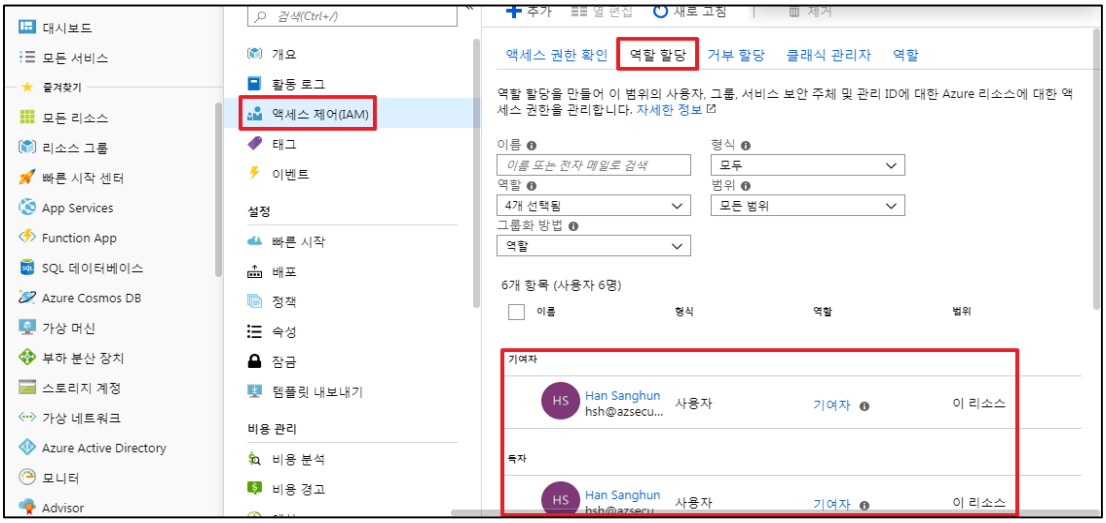
3) 추가할 역할/권한 선택



4) 역할/권한을 설정할 사용자 선택



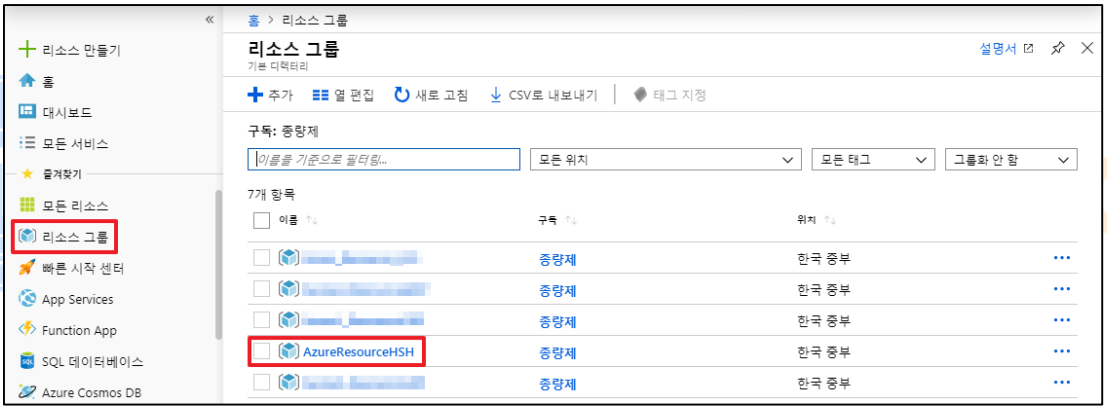
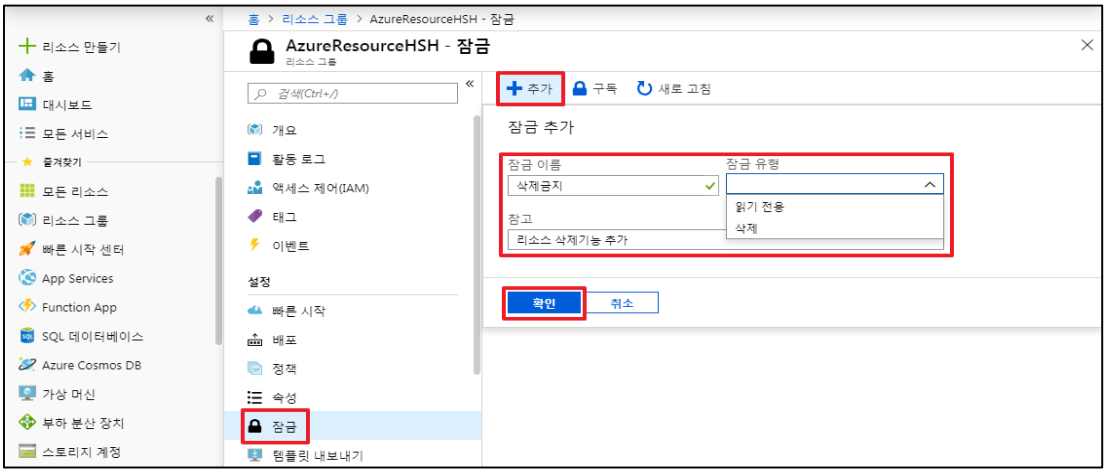
5) 액세스 제어(IAM) 메뉴 내 역할 할당 메뉴에서 설정된 역할/권한 및 계정 확인

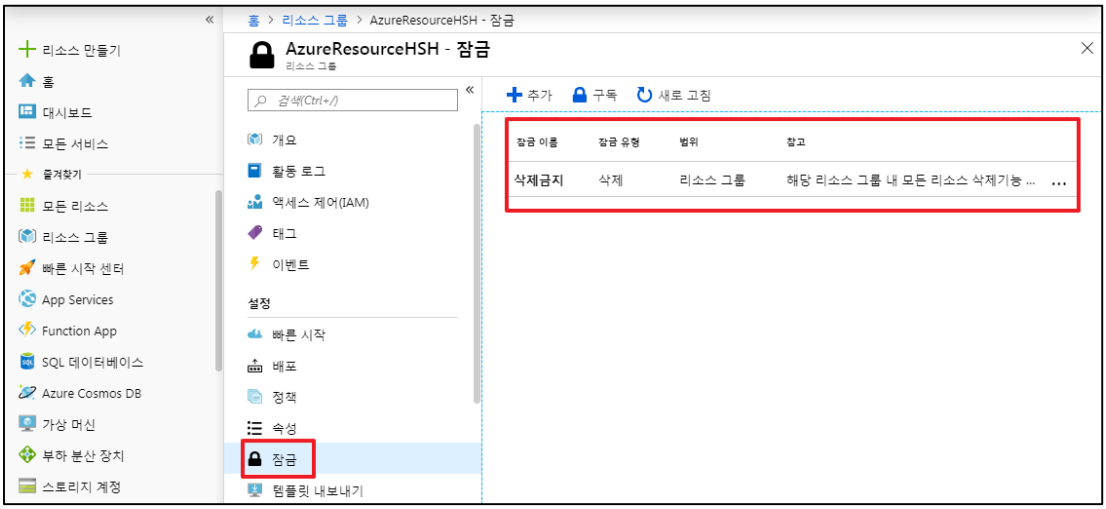


진단 기준	양호기준 : 리소스 그룹 내 관리목적에 불필요한 리소스가 포함되지 않은 경우

	취약기준 : 리소스 그룹 내 관리목적에 불필요한 리소스가 포함되어 있을 경우
비고	

1.2 리소스 그룹 잠금

분류	권한관리	중요도	중
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 잠금수준** - 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** : 관리되고 있는 리소스 그룹의 잠금기능을 설정하여 사용하고 있을 경우 **취약기준** : 관리되고 있는 리소스 그룹의 잠금기능을 설정하여 사용하고 있지 않을 경우
비고	

1.3 액세스 제어(IAM) 최고 권한 역할 할당

분류	권한관리	중요도	상
항목명	액세스 제어(IAM) 최고 권한 역할 할당		

항목 설명

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

※ IAM 사용자 역할

역할 이름 (한글)	역할 이름 (영문)	상세설명
소유자	Owner	리소스 액세스를 비롯한 모든 것을 관리함
기여자	Contributor	리소스 액세스를 제외한 모든 것을 관리함
독자	Reader	모든 항목을 볼 수 있지만 변경할 수 있는 권한은 없음
Avere 연산자	Avere Contributor	Avere vFXT 클러스터에서 클러스터를 관리함
Avere 참가자	Avere Operator	Avere vFXT 클러스터를 만들고 관리함
DevTest Labs 사용자	DevTest Labs User	Azure DevTest Labs 의 가상 머신 연결, 시작, 다시 시작 및 종료할 수 있음
Log Analytics 독자	Log Analytics Reader	Log Analytics 독자는 모든 Azure 리소스에 대한 Azure Diagnostics 의 구성 보기를 비롯하여 모니터링 설정 보기 및 모든 모니터링 데이터를 보고 검색할 수 있음
Log Analytics 참가자	Log Analytics Contributor	Log Analytics 참가자는 모든 모니터링 데이터를 읽고 모니터링 설정을 편집할 수 있습니다. 모니터링 설정 편집에는 VM 에 VM 확장 추가, Azure Storage 에서 로그 컬렉션을 구성할 수 있는 스토리지 계정 키 읽기, Automation 계정 생성 및 구성, 솔루션 추가 및 모든 Azure 리소스에 대한 Azure Diagnostics 을 구성하는 기능도 포함되어 있습니다.
Logic Apps 참가자	Logic App Contributor	Logic Apps 을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음
Site Recovery 운영자	Site Recovery Operator	장애 조치(failover) 및 장애 복구(failback)를 수행할 수 있지만 다른 Site Recovery 관리 작업은 수행할 수 없음
Site Recovery 참가자	Site Recovery Contributor	자격 증명 모음 만들기 및 역할 할당을 제외한 Site Recovery 서비스를 관리할 수 있음
Storage Blob 데이터	Storage Blob Data Contributor	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기, 쓰기 및 삭제 액세스를 허용

Contributor		
Storage Blob 데이터 Reader	Storage Blob Data Reader	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기 액세스를 허용
Storage Blob 데이터 소유자	Storage Blob Data Owner	POSIX 액세스 제어 할당을 포함하여 Azure Storage Blob 컨테이너 및 데이터에 대한 모든 권한 허용
Storage 계정 참가자	Storage Account Contributor	Storage 계정을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음
Storage 큐 데이터 Contributor	Storage Queue Data Contributor	Azure Storage 큐 및 큐 메시지에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage 큐 데이터 Reader	Storage Queue Data Reader	Azure Storage 큐 및 큐 메시지에 대한 읽기 액세스를 허용
Storage 큐 데이터 메시지 보낸 사람	Storage Queue Data Message Sender	Azure Storage 큐 메시지 보내기 허용
Storage 큐 데이터 메시지 프로세서	Storage Queue Data Message Processor	Azure Storage 큐 메시지에 대한 미리 보기, 수신 및 삭제 권한 허용
가상 머신 참가자	Virtual Machine Contributor	가상 컴퓨터를 관리할 수 있지만 가상 컴퓨터나 가상 컴퓨터가 연결된 가상 네트워크 또는 저장소 계정에 액세스 할 수 없음
관리되는 애플리케이션 운영자 역할	Managed Application Operator Role	관리되는 애플리케이션 리소스에서 작업을 읽고 수행할 수 있음
관리되는 애플리케이션 판독기	Managed Application Reader	관리되는 앱에서 리소스를 읽고 JIT 액세스 권한을 요청할 수 있음
리소스 정책 참가자(미리 보기)	Resource Policy Contributor (Preview)	(미리 보기) 리소스 정책을 생성/수정하고, 지원 티켓을 만들고, 리소스/계층 구조를 읽을 수 있는 권한을 가진 EA 의 백필된 사용자
모니터링 리더	Monitoring Reader	모든 모니터링 데이터를 읽을 수 있음
모니터링 메트릭 게시자	Monitoring Metrics Publisher	Azure 리소스에 대해 메트릭을 게시할 수 있음
모니터링 참가자	Monitoring Contributor	모든 모니터링 데이터를 읽고 모니터링 설정을 업데이트할 수 있음
백업 운영자	Backup Operator	백업 제거를 제외한 백업 서비스를 관리하고 자격 증명 모음 만들고 다른 사람에게 액세스 권한을 부여할 수 있음

백업 참가자	Backup Contributor	백업 서비스를 관리할 수 있지만, 자격 증명 모음을 만들고 다른 사용자에게 액세스 권한을 부여할 수 없음
사용자 액세스 관리자	User Access Administrator	Azure 리소스에 대한 사용자 액세스를 관리할 수 있음
스토리지 계정 키 운영자 서비스 역할	Storage Account Key Operator Service Role	스토리지 계정 키 운영자가 스토리지 계정에서 키를 나열하고 다시 생성할 수 있음
읽기 권한자 및 데이터 액세스	Reader and Data Access	모든 항목을 볼 수 있지만, 스토리지 계정 또는 포함된 리소스를 삭제하거나 만들 수는 없고, 스토리지 계정 키에 액세스하면 스토리지 계정에 포함된 모든 데이터에 대한 읽기/쓰기 액세스가 허용됩니다.

※ IAM 역할별 권한 관리 (예시)

역할	IAM 관리형 정책명
Console 관리자	Owner(소유자)
Infra 관리자	Contridutor(기여자), Site Recovery Contributor(Site Recovery 참가자), Backup Operator(백업 운영자), User Access Administrator(사용자 액세스 관리자)
Infra 운영 및 담당자	Reader(독자), DevTest Labs User(DevTest Labs 사용자), Virtual Machine Contributor(가상 머신 참가자), Site Recovery Operator(Site Recovery 운영자), Backup Contributor(백업 참가자)
Application 관리자	Managed Application Operator Role(관리되는 애플리케이션 운영자 역할)
Application 운영 및 담당자	Logic App Contributor(Logic Apps 참가자), Managed Application Reader(관리되는 애플리케이션 판독기)
개발 관리자	Storage Blob Data Owner(Storage Blob 데이터 소유자), Storage Queue Data Contributor(Storage 큐 데이터 Contributor)
개발 운영 및 담당자	Storage Blob Data Contributor(Storage Blob 데이터 Contributor), Storage Blob Data Reader(Storage Blob 데이터 Reader), Storage Account Contributor(Storage 계정 참가자), Storage Queue Data Message Processor(Storage 큐 데이터 메시지 프로세서), Storage Queue Data Message Sender(Storage 큐 데이터 메시지 보낸 사람), Storage Queue Data Reader(Storage 큐 데이터 Reader), Storage Account Key Operator Service Role(스토리지 계정 키 운영자 서비스 역할)

보안 관리자	Log Analytics Contributor(Log Analytics 참가자), Resource Policy Contributor (리소스 정책 참가자(미리 보기)), User Access Administrator(사용자 액세스 관리자)
보안 운영 및 담당자	Log Analytics Reader(Log Analytics 독자), Storage Account Key Operator Service Role(스토리지 계정 키 운영자 서비스 역할)
로깅 관리자	Monitoring Contributor(모니터링 참가자)
로깅 운영 및 담당자	Monitoring Reader(모니터링 리더), Monitoring Metrics Publisher(모니터링 메트릭 게시자)
재무/비용 관리자	Reader and Data Access(읽기 권한자 및 데이터 액세스)

※ IAM 관리형 정책 권한 관리 List (예시)

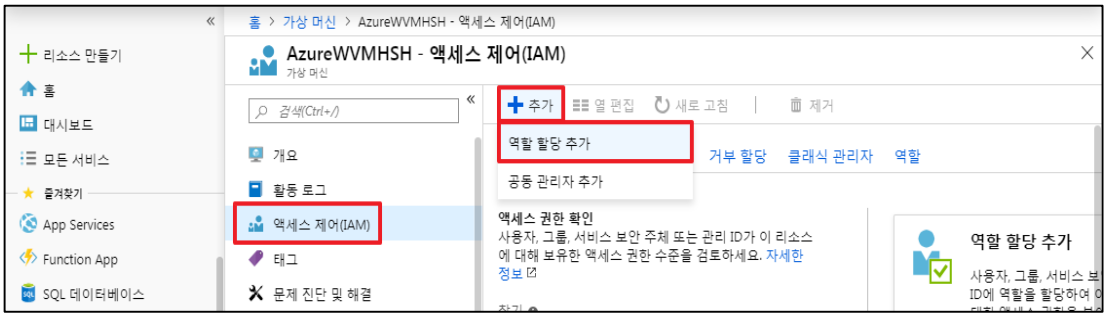
역할	계정 관리 (그룹 및 계정명)	관리형 정책	취약 유/무
Console 관리자	Ex)Owner(소유자)	Ex)Owner(소유자)	N/A
Infra 관리자/운영 및 담당자			N/A
Application 관리자/ 운영 및 담당자			N/A
개발 관리자/ 운영 및 담당자			N/A
재무 / 비용 관리자 및 담당자			N/A

설정 방법

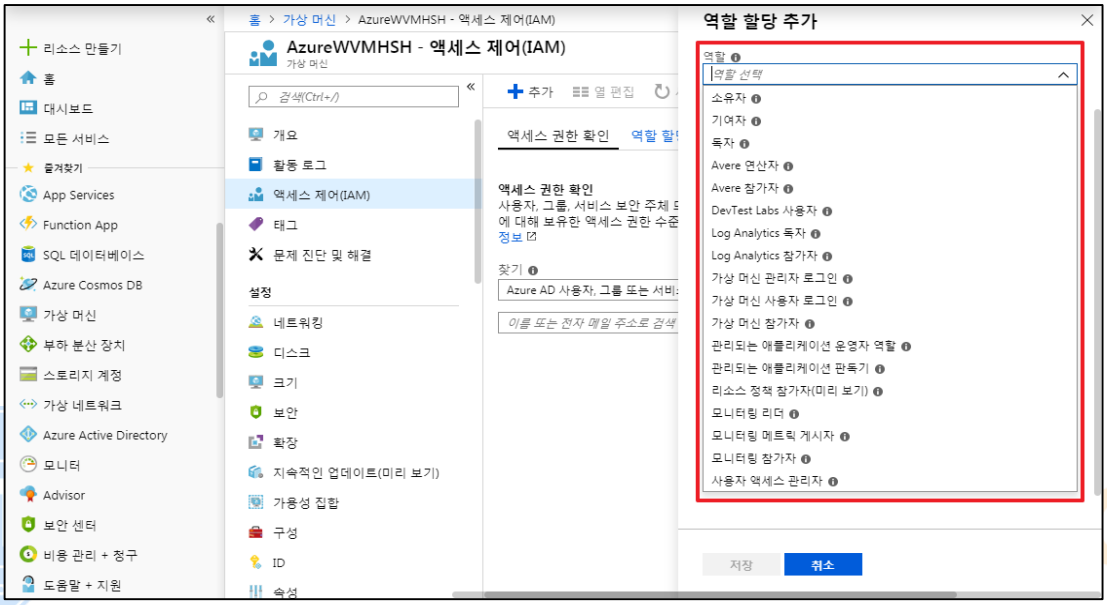
가. 리소스 내 액세스 제어(IAM) 설정 방법

1) 액세스 제어를 설정할 리소스 선택

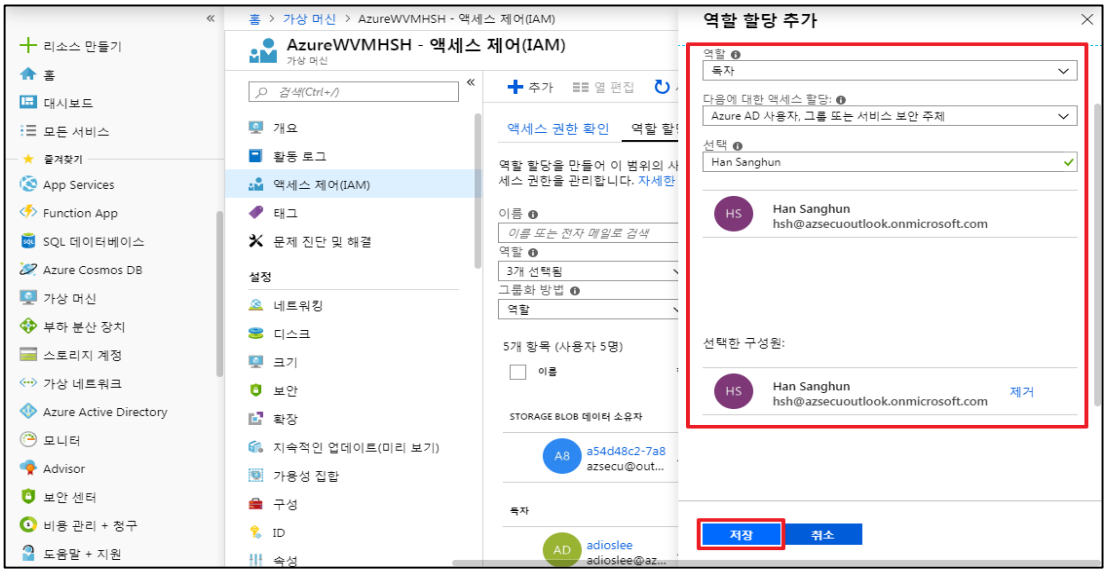
2) 리소스 내 액세스 제어(IAM) 선택 후 역할 할당 추가 버튼 클릭



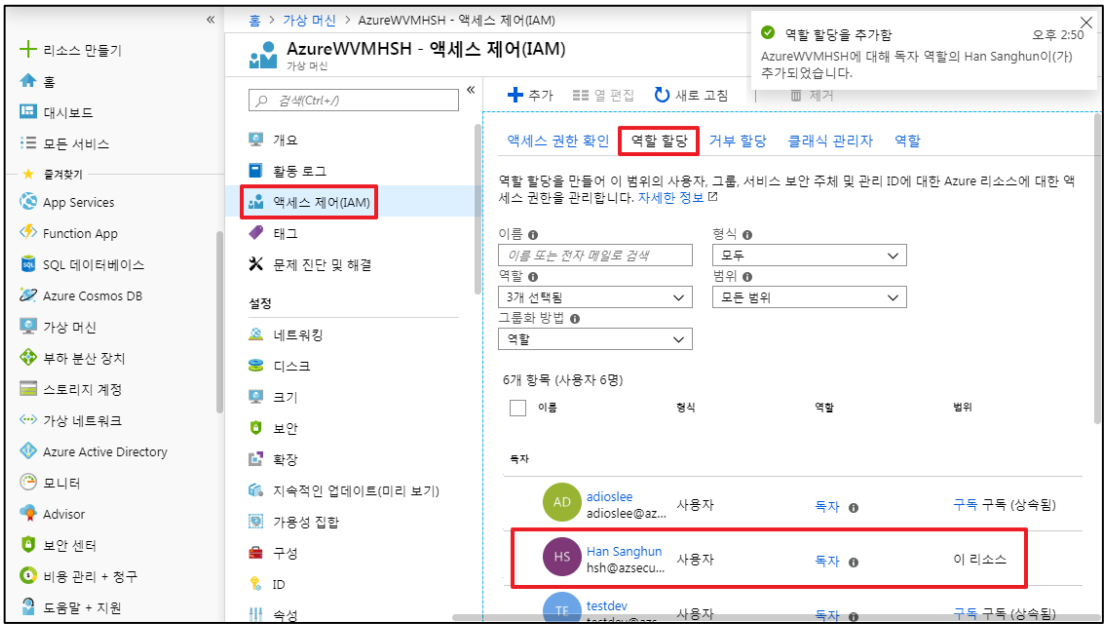
3) 추가할 역할/권한 선택



4) 역할/권한을 설정할 사용자 선택



5) 액세스 제어(IAM) 메뉴 내 역할 할당 메뉴에서 설정된 역할/권한 및 계정 확인

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: "소유자/기여자/사용자 액세스 관리자" 권한이 최고 관리자에게만 부여된 경우

취약기준
: "소유자/기여자/사용자 액세스 관리자" 권한이 일반 사용자에게 부여된 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

1.4 액세스 제어(IAM) 역할 할당

<table>
<tr><td>분류</td><td>권한관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">액세스 제어(IAM) 역할 할당</td></tr>
<tr><td>항목
설명</td><td colspan="3">클라우드 리소스에 대한 액세스 관리는 클라우드를 사용하는 모든 조직에서 중요한 기능입니다. RBAC(역할 기반 액세스 제어)는 Azure 리소스에 액세스할 수 있는 사용자, 해당 리소스로 수행할 수 있는 작업 및 액세스 권한이 있는 영역을 관리하는 데 도움을 줍니다.
RBAC 는 Azure 리소스에 대한 액세스를 세밀하게 관리할 수 있는 Azure Resource Manager 기반의 권한 부여 시스템입니다.

※ IAM 사용자 역할
<table>
<tr><th>역할 이름
(한글)</th><th>역할 이름
(영문)</th><th>상세설명</th></tr>
<tr><td>소유자</td><td>Owner</td><td>리소스 액세스를 비롯한 모든 것을 관리함</td></tr>
<tr><td>기여자</td><td>Contributor</td><td>리소스 액세스를 제외한 모든 것을 관리함</td></tr>
<tr><td>독자</td><td>Reader</td><td>모든 항목을 볼 수 있지만 변경할 수 있는 권한은 없음</td></tr>
<tr><td>Avere 연산자</td><td>Avere Contributor</td><td>Avere vFXT 클러스터에서 클러스터를 관리함</td></tr>
<tr><td>Avere 참가자</td><td>Avere Operator</td><td>Avere vFXT 클러스터를 만들고 관리함</td></tr>
<tr><td>DevTest Labs 사용자</td><td>DevTest Labs User</td><td>Azure DevTest Labs 의 가상 머신 연결, 시작, 다시 시작 및 종료할 수 있음</td></tr>
<tr><td>Log Analytics 독자</td><td>Log Analytics Reader</td><td>Log Analytics 독자는 모든 Azure 리소스에 대한 Azure Diagnostics 의 구성 보기를 비롯하여 모니터링 설정 보기 및 모든 모니터링 데이터를 보고 검색할 수 있음</td></tr>
<tr><td>Log Analytics 참가자</td><td>Log Analytics Contributor</td><td>Log Analytics 참가자는 모든 모니터링 데이터를 읽고 모니터링 설정을 편집할 수 있습니다. 모니터링 설정 편집에는 VM 에 VM 확장 추가,
Azure Storage 에서 로그 컬렉션을 구성할 수 있는 스토리지 계정 키 읽기, Automation 계정 생성 및 구성, 솔루션 추가 및
모든 Azure 리소스에 대한 Azure Diagnostics 을 구성하는 기능도 포함되어 있습니다.</td></tr>
<tr><td>Logic Apps 참가자</td><td>Logic App Contributor</td><td>Logic Apps 을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음</td></tr>
<tr><td>Site Recovery 운영자</td><td>Site Recovery Operator</td><td>장애 조치(failover) 및 장애 복구(failback)를 수행할 수 있지만 다른 Site Recovery 관리 작업은 수행할 수 없음</td></tr>
<tr><td>Site Recovery 참가자</td><td>Site Recovery Contributor</td><td>자격 증명 모음 만들기 및 역할 할당을 제외한 Site Recovery 서비스를 관리할 수 있음</td></tr>
</table>
</td></tr>
</table>

Storage Blob 데이터 Contributor	Storage Blob Data Contributor	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage Blob 데이터 Reader	Storage Blob Data Reader	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기 액세스를 허용
Storage Blob 데이터 소유자	Storage Blob Data Owner	POSIX 액세스 제어 할당을 포함하여 Azure Storage Blob 컨테이너 및 데이터에 대한 모든 권한 허용
Storage 계정 참가자	Storage Account Contributor	Storage 계정을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음
Storage 큐 데이터 Contributor	Storage Queue Data Contributor	Azure Storage 큐 및 큐 메시지에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage 큐 데이터 Reader	Storage Queue Data Reader	Azure Storage 큐 및 큐 메시지에 대한 읽기 액세스를 허용
Storage 큐 데이터 메시지 보낸 사람	Storage Queue Data Message Sender	Azure Storage 큐 메시지 보내기 허용
Storage 큐 데이터 메시지 프로세서	Storage Queue Data Message Processor	Azure Storage 큐 메시지에 대한 미리 보기, 수신 및 삭제 권한 허용
가상 머신 참가자	Virtual Machine Contributor	가상 컴퓨터를 관리할 수 있지만 가상 컴퓨터나 가상 컴퓨터가 연결된 가상 네트워크 또는 저장소 계정에 액세스 할 수 없음
관리되는 애플리케이션 운영자 역할	Managed Application Operator Role	관리되는 애플리케이션 리소스에서 작업을 읽고 수행할 수 있음
관리되는 애플리케이션 판독기	Managed Application Reader	관리되는 앱에서 리소스를 읽고 JIT 액세스 권한을 요청할 수 있음
리소스 정책 참가자(미리 보기)	Resource Policy Contributor (Preview)	(미리 보기) 리소스 정책을 생성/수정하고, 지원 티켓을 만들고, 리소스/계층 구조를 읽을 수 있는 권한을 가진 EA 의 백필된 사용자
모니터링 리더	Monitoring Reader	모든 모니터링 데이터를 읽을 수 있음
모니터링 메트릭 게시자	Monitoring Metrics Publisher	Azure 리소스에 대해 메트릭을 게시할 수 있음
모니터링 참가자	Monitoring Contributor	모든 모니터링 데이터를 읽고 모니터링 설정을 업데이트할 수 있음
백업 운영자	Backup Operator	백업 제거를 제외한 백업 서비스를 관리하고 자격

		증명 모음 만들고 다른 사람에게 액세스 권한을 부여할 수 있음
백업 참가자	Backup Contributor	백업 서비스를 관리할 수 있지만, 자격 증명 모음을 만들고 다른 사용자에게 액세스 권한을 부여할 수 없음
사용자 액세스 관리자	User Access Administrator	Azure 리소스에 대한 사용자 액세스를 관리할 수 있음
스토리지 계정 키 운영자 서비스 역할	Storage Account Key Operator Service Role	스토리지 계정 키 운영자가 스토리지 계정에서 키를 나열하고 다시 생성할 수 있음
읽기 권한자 및 데이터 액세스	Reader and Data Access	모든 항목을 볼 수 있지만, 스토리지 계정 또는 포함된 리소스를 삭제하거나 만들 수는 없고, 스토리지 계정 키에 액세스하면 스토리지 계정에 포함된 모든 데이터에 대한 읽기/쓰기 액세스가 허용됩니다.

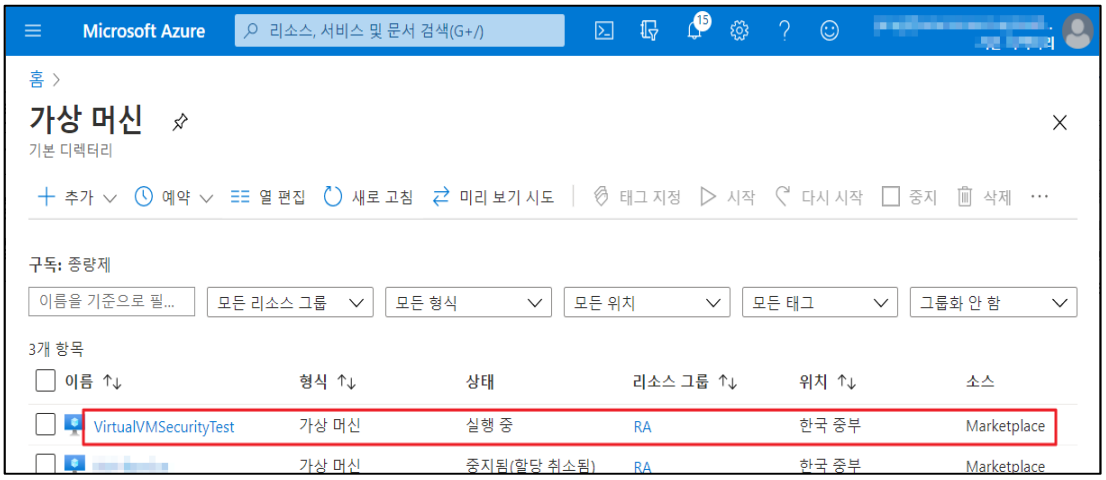
※ IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	관리형 정책	취약 유/무
Console 관리자	Ex)Owner(소유자)	Ex)Owner(소유자)	N/A
Infra 관리자/운영 및 담당자			N/A
Application 관리자/ 운영 및 담당자			N/A
개발 관리자/ 운영 및 담당자			N/A
재무 / 비용 관리자 및 담당자			N/A

설정 방법

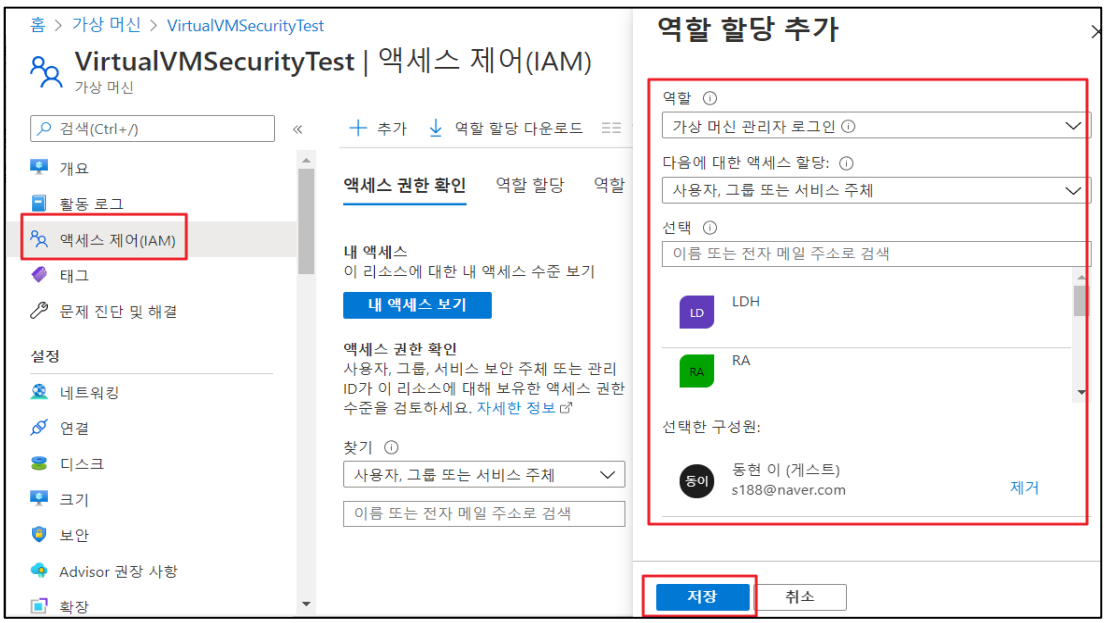
가. 가상머신 역할 설정

1) 가상머신 역할 추가



2-1) 가상머신 액세스 제어(IAM) 역할 추가

2-2) 가상머신 액세스 제어(IAM) 역할 추가



3) 추가된 액세스 제어(IAM) 확인

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


나. 가상머신 액세스 제어(IAM) 역할 확인

1) 액세스 제어(IAM) 확인

</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: IAM 사용자의 권한/그룹을 목적에 맞게 역할을 할당하고 있을 경우

취약기준
: IAM 사용자의 권한/그룹을 목적에 맞게 역할을 할당하고 있지 않을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

1.5 AD 관리자 역할 할당

분류	권한관리	중요도	상
항목명	AD 관리자 역할 할당		

항목 설명

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 관리목적에 맞게 역할을 할당해야 합니다.

※ Azure AD 관리역할

역할 이름 (한글)	역할 이름 (영문)	상세설명
소유자	Owner	리소스 액세스를 비롯한 모든 것을 관리함
기여자	Contributor	리소스 액세스를 제외한 모든 것을 관리함
독자	Reader	모든 항목을 볼 수 있지만 변경할 수 있는 권한은 없음
Avere 연산자	Avere Contributor	Avere vFXT 클러스터에서 클러스터를 관리함
Avere 참가자	Avere Operator	Avere vFXT 클러스터를 만들고 관리함
DevTest Labs 사용자	DevTest Labs User	Azure DevTest Labs 의 가상 머신 연결, 시작, 다시 시작 및 종료할 수 있음
Log Analytics 독자	Log Analytics Reader	Log Analytics 독자는 모든 Azure 리소스에 대한 Azure Diagnostics 의 구성 보기를 비롯하여 모니터링 설정 보기 및 모든 모니터링 데이터를 보고 검색할 수 있음
Log Analytics 참가자	Log Analytics Contributor	Log Analytics 참가자는 모든 모니터링 데이터를 읽고 모니터링 설정을 편집할 수 있습니다. 모니터링 설정 편집에는 VM 에 VM 확장 추가, Azure Storage 에서 로그 컬렉션을 구성할 수 있는 스토리지 계정 키 읽기, Automation 계정 생성 및 구성, 솔루션 추가 및 모든 Azure 리소스에 대한 Azure Diagnostics 을 구성하는 기능도 포함되어 있습니다.
Logic Apps 참가자	Logic App Contributor	Logic Apps 을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음
Site Recovery 운영자	Site Recovery Operator	장애 조치(failover) 및 장애 복구(failback)를 수행할 수 있지만 다른 Site Recovery 관리 작업은 수행할 수 없음
Site Recovery 참가자	Site Recovery Contributor	자격 증명 모음 만들기 및 역할 할당을 제외한 Site Recovery 서비스를 관리할 수 있음
Storage Blob	Storage Blob	Azure Storage Blob 컨테이너 및 데이터에 대한

데이터 Contributor	Data Contributor	읽기, 쓰기 및 삭제 액세스를 허용
Storage Blob 데이터 Reader	Storage Blob Data Reader	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기 액세스를 허용
Storage Blob 데이터 소유자	Storage Blob Data Owner	POSIX 액세스 제어 할당을 포함하여 Azure Storage Blob 컨테이너 및 데이터에 대한 모든 권한 허용
Storage 계정 참가자	Storage Account Contributor	Storage 계정을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음
Storage 큐 데이터 Contributor	Storage Queue Data Contributor	Azure Storage 큐 및 큐 메시지에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage 큐 데이터 Reader	Storage Queue Data Reader	Azure Storage 큐 및 큐 메시지에 대한 읽기 액세스를 허용
Storage 큐 데이터 메시지 보낸 사람	Storage Queue Data Message Sender	Azure Storage 큐 메시지 보내기 허용
Storage 큐 데이터 메시지 프로세서	Storage Queue Data Message Processor	Azure Storage 큐 메시지에 대한 미리 보기, 수신 및 삭제 권한 허용
가상 머신 참가자	Virtual Machine Contributor	가상 컴퓨터를 관리할 수 있지만 가상 컴퓨터나 가상 컴퓨터가 연결된 가상 네트워크 또는 저장소 계정에 액세스 할 수 없음
관리되는 애플리케이션 운영자 역할	Managed Application Operator Role	관리되는 애플리케이션 리소스에서 작업을 읽고 수행할 수 있음
관리되는 애플리케이션 판독기	Managed Application Reader	관리되는 앱에서 리소스를 읽고 JIT 액세스 권한을 요청할 수 있음
리소스 정책 참가자(미리 보기)	Resource Policy Contributor (Preview)	(미리 보기) 리소스 정책을 생성/수정하고, 지원 티켓을 만들고, 리소스/계층 구조를 읽을 수 있는 권한을 가진 EA 의 백필된 사용자
모니터링 리더	Monitoring Reader	모든 모니터링 데이터를 읽을 수 있음
모니터링 메트릭 게시자	Monitoring Metrics Publisher	Azure 리소스에 대해 메트릭을 게시할 수 있음
모니터링 참가자	Monitoring Contributor	모든 모니터링 데이터를 읽고 모니터링 설정을 업데이트할 수 있음
백업 운영자	Backup Operator	백업 제거를 제외한 백업 서비스를 관리하고 자격 증명 모음 만들고 다른 사람에게 액세스 권한을

		부여할 수 있음
백업 참가자	Backup Contributor	백업 서비스를 관리할 수 있지만, 자격 증명 모음을 만들고 다른 사용자에게 액세스 권한을 부여할 수 없음
사용자 액세스 관리자	User Access Administrator	Azure 리소스에 대한 사용자 액세스를 관리할 수 있음
스토리지 계정 키 운영자 서비스 역할	Storage Account Key Operator Service Role	스토리지 계정 키 운영자가 스토리지 계정에서 키를 나열하고 다시 생성할 수 있음
읽기 권한자 및 데이터 액세스	Reader and Data Access	모든 항목을 볼 수 있지만, 스토리지 계정 또는 포함된 리소스를 삭제하거나 만들 수는 없고, 스토리지 계정 키에 액세스하면 스토리지 계정에 포함된 모든 데이터에 대한 읽기/쓰기 액세스가 허용됩니다.

※ Azure AD 관리자 역할 (예시)

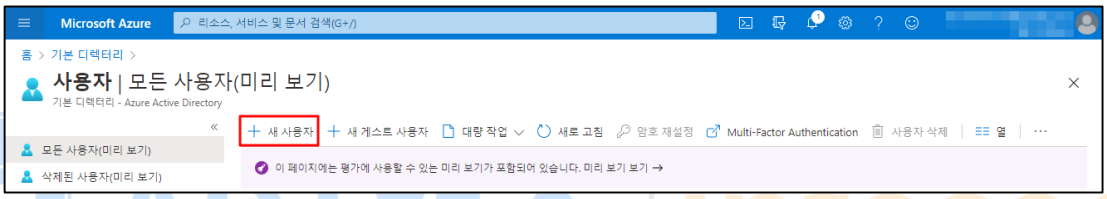
역할	AD 관리자 역할
Console 관리자	Global administrator(전역 관리자)
Infra 관리자	Authentication administrator(인증 관리자), User administrator(사용자 관리자), Cloud device administrator(클라우드 디바이스 관리자), License administrator(라이선스 관리자)
Infra 운영 및 담당자	Conditional Access administrator(조건부 액세스 관리자), Helpdesk (Password) administrator(기술 지원팀(암호) 관리자)
Application 관리자	Service administrator(서비스 관리자), Application administrator(애플리케이션 관리자), Cloud application administrator(클라우드 애플리케이션 관리자)
Application 운영 및 담당자	Application developer(애플리케이션 개발자)
개발 관리자	Service administrator(서비스 관리자), Application administrator(애플리케이션 관리자), Cloud application administrator(클라우드 애플리케이션 관리자)
개발 운영 및 담당자	Application developer(애플리케이션 개발자)
보안 관리자	Security administrator(보안 관리자), Privileged role administrator(권한 있는 역할 관리자), Privileged

	authentication administrator(권한 있는 인증 관리자), Reports reader(보고서 읽기 권한자), Guest inviter(게스트 초대자)
보안 운영 및 담당자	Security operator(보안 운영자), Security reader(보안 읽기 권한자), Compliance administrator(준수 관리자), Compliance data administrator(준수 데이터 관리자)
로깅 관리자	Desktop Analytics administrator(데스크톱 분석 관리자), Azure Information Protection administrator(Azure Information Protection 관리자), B2C user flow attribute administrator(B2C 사용자 흐름 특성 관리자)
로깅 운영 및 담당자	B2C user flow administrator(B2C 사용자 흐름 관리자),
재무/비용 관리자	Billing administrator(대금 청구 관리자), Message center privacy reader(메시지 센터 프라이버시 읽기 권한자)

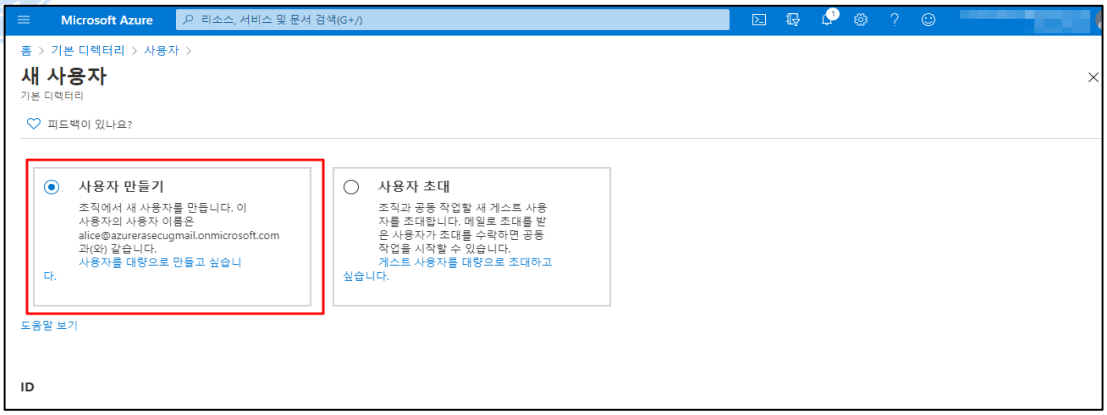
설정 방법

가. Active Directory 사용자 생성 및 관리자 권한 부여

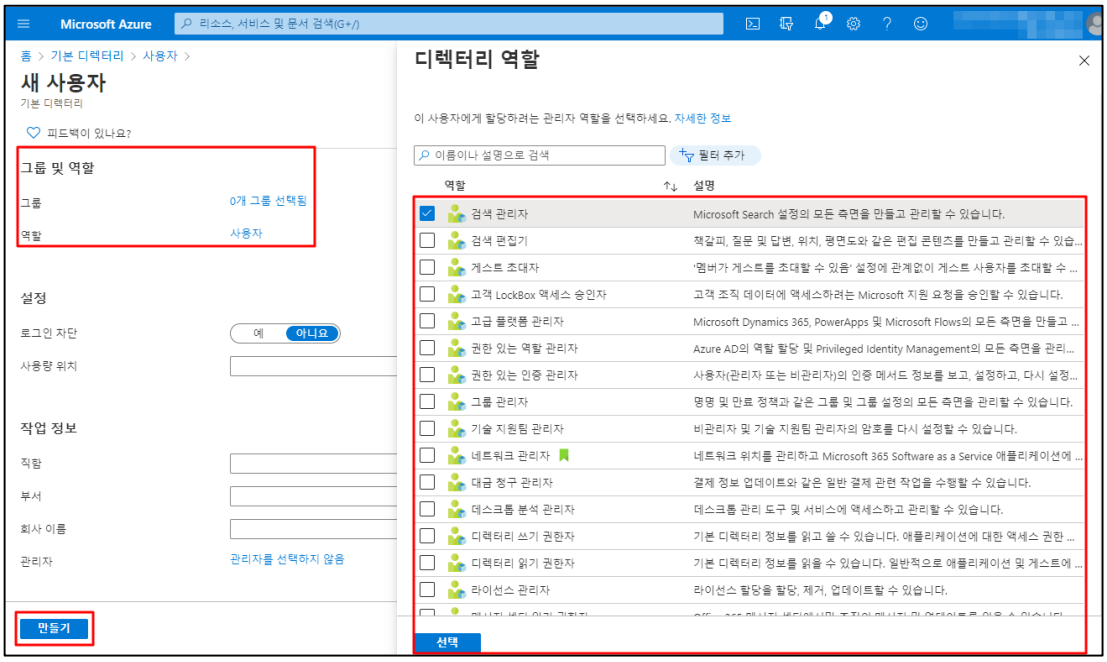
1) 새 사용자 추가



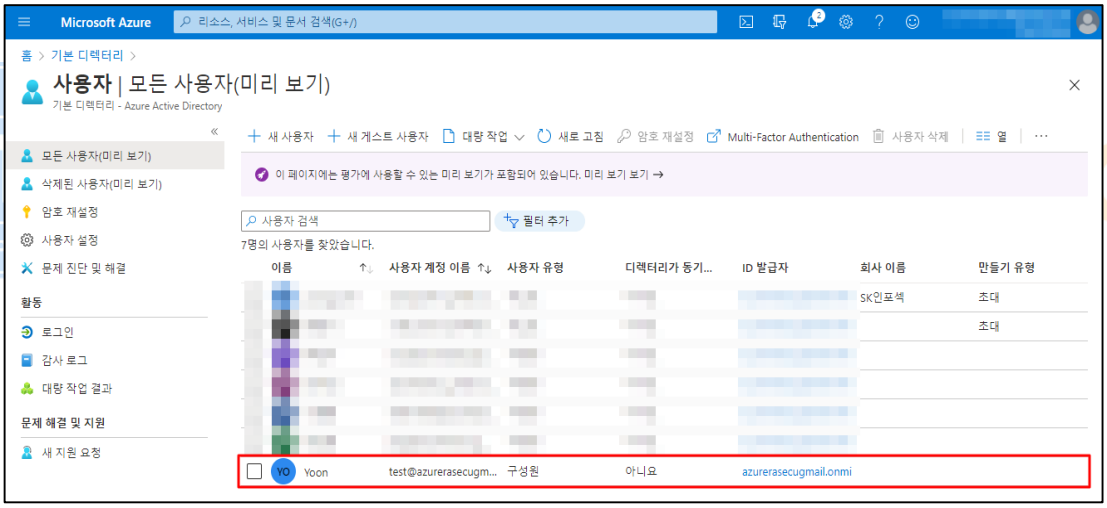
2) 사용자 만들기 및 계정 정보 입력



3) 단일 관리자 역할 할당



4) 역할 할당된 단일 사용자 추가 확인



진단 기준	**양호기준** : 관리자 역할에 단일 사용자 계정이 할당되어 있을 경우 **취약기준** : 관리자 역할에 단일 사용자 계정이 할당되어 있지 않을 경우
비고	

1.6 AD 일반 계정 역할 할당

<table>
<tr><td>분류</td><td>권한관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">AD 일반 계정 역할 할당</td></tr>
<tr><td>항목
설명</td><td colspan="3">Active Directory 사용자 별 관리 역할이 구분되어 있고 관련 역할은 Active Directory의 계정 관리를 위해 존재합니다. 역할 및 관리자 기능은 Active Directory 및 기타 Microsoft 서비스에 대한 액세스 권한을 부여하는데 사용할 수 있습니다.

※ Azure AD 관리역할
<table>
<tr><th>역할 이름
(한글)</th><th>역할 이름
(영문)</th><th>상세설명</th></tr>
<tr><td>소유자</td><td>Owner</td><td>리소스 액세스를 비롯한 모든 것을 관리함</td></tr>
<tr><td>기여자</td><td>Contributor</td><td>리소스 액세스를 제외한 모든 것을 관리함</td></tr>
<tr><td>독자</td><td>Reader</td><td>모든 항목을 볼 수 있지만 변경할 수 있는 권한은 없음</td></tr>
<tr><td>Avere 연산자</td><td>Avere Contributor</td><td>Avere vFXT 클러스터에서 클러스터를 관리함</td></tr>
<tr><td>Avere 참가자</td><td>Avere Operator</td><td>Avere vFXT 클러스터를 만들고 관리함</td></tr>
<tr><td>DevTest Labs 사용자</td><td>DevTest Labs User</td><td>Azure DevTest Labs 의 가상 머신 연결, 시작, 다시 시작 및 종료할 수 있음</td></tr>
<tr><td>Log Analytics 독자</td><td>Log Analytics Reader</td><td>Log Analytics 독자는 모든 Azure 리소스에 대한 Azure Diagnostics 의 구성 보기를 비롯하여 모니터링 설정 보기 및 모든 모니터링 데이터를 보고 검색할 수 있음</td></tr>
<tr><td>Log Analytics 참가자</td><td>Log Analytics Contributor</td><td>Log Analytics 참가자는 모든 모니터링 데이터를 읽고 모니터링 설정을 편집할 수 있습니다. 모니터링 설정 편집에는 VM 에 VM 확장 추가,
Azure Storage 에서 로그 컬렉션을 구성할 수 있는 스토리지 계정 키 읽기, Automation 계정 생성 및 구성, 솔루션 추가 및
모든 Azure 리소스에 대한 Azure Diagnostics 을 구성하는 기능도 포함되어 있습니다.</td></tr>
<tr><td>Logic Apps 참가자</td><td>Logic App Contributor</td><td>Logic Apps 을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음</td></tr>
<tr><td>Site Recovery 운영자</td><td>Site Recovery Operator</td><td>장애 조치(failover) 및 장애 복구(failback)를 수행할 수 있지만 다른 Site Recovery 관리 작업은 수행할 수 없음</td></tr>
<tr><td>Site Recovery 참가자</td><td>Site Recovery Contributor</td><td>자격 증명 모음 만들기 및 역할 할당을 제외한 Site Recovery 서비스를 관리할 수 있음</td></tr>
<tr><td>Storage Blob 데이터</td><td>Storage Blob Data Contributor</td><td>Azure Storage Blob 컨테이너 및 데이터에 대한 읽기, 쓰기 및 삭제 액세스를 허용</td></tr>
</table>
</td></tr>
</table>

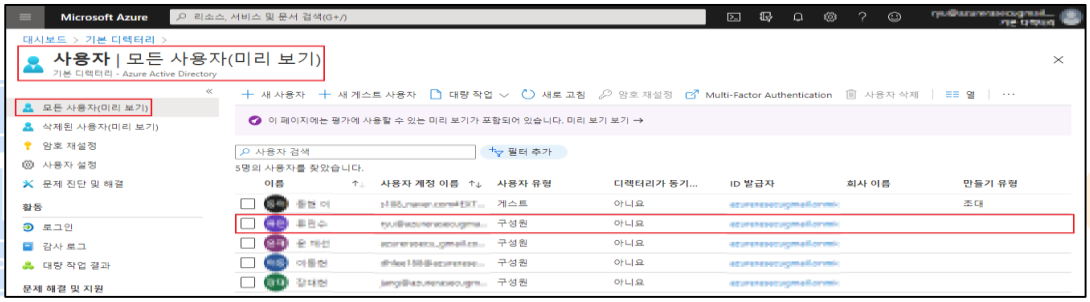
Contributor		
Storage Blob 데이터 Reader	Storage Blob Data Reader	Azure Storage Blob 컨테이너 및 데이터에 대한 읽기 액세스를 허용
Storage Blob 데이터 소유자	Storage Blob Data Owner	POSIX 액세스 제어 할당을 포함하여 Azure Storage Blob 컨테이너 및 데이터에 대한 모든 권한 허용
Storage 계정 참가자	Storage Account Contributor	Storage 계정을 관리할 수 있지만 해당 리소스에는 액세스 할 수 없음
Storage 큐 데이터 Contributor	Storage Queue Data Contributor	Azure Storage 큐 및 큐 메시지에 대한 읽기, 쓰기 및 삭제 액세스를 허용
Storage 큐 데이터 Reader	Storage Queue Data Reader	Azure Storage 큐 및 큐 메시지에 대한 읽기 액세스를 허용
Storage 큐 데이터 메시지 보낸 사람	Storage Queue Data Message Sender	Azure Storage 큐 메시지 보내기 허용
Storage 큐 데이터 메시지 프로세서	Storage Queue Data Message Processor	Azure Storage 큐 메시지에 대한 미리 보기, 수신 및 삭제 권한 허용
가상 머신 참가자	Virtual Machine Contributor	가상 컴퓨터를 관리할 수 있지만 가상 컴퓨터나 가상 컴퓨터가 연결된 가상 네트워크 또는 저장소 계정에 액세스 할 수 없음
관리되는 애플리케이션 운영자 역할	Managed Application Operator Role	관리되는 애플리케이션 리소스에서 작업을 읽고 수행할 수 있음
관리되는 애플리케이션 판독기	Managed Application Reader	관리되는 앱에서 리소스를 읽고 JIT 액세스 권한을 요청할 수 있음
리소스 정책 참가자(미리 보기)	Resource Policy Contributor (Preview)	(미리 보기) 리소스 정책을 생성/수정하고, 지원 티켓을 만들고, 리소스/계층 구조를 읽을 수 있는 권한을 가진 EA 의 백필된 사용자
모니터링 리더	Monitoring Reader	모든 모니터링 데이터를 읽을 수 있음
모니터링 메트릭 게시자	Monitoring Metrics Publisher	Azure 리소스에 대해 메트릭을 게시할 수 있음
모니터링 참가자	Monitoring Contributor	모든 모니터링 데이터를 읽고 모니터링 설정을 업데이트할 수 있음
백업 운영자	Backup Operator	백업 제거를 제외한 백업 서비스를 관리하고 자격 증명 모음 만들고 다른 사람에게 액세스 권한을 부여할 수 있음

백업 참가자	Backup Contributor	백업 서비스를 관리할 수 있지만, 자격 증명 모음을 만들고 다른 사용자에게 액세스 권한을 부여할 수 없음
사용자 액세스 관리자	User Access Administrator	Azure 리소스에 대한 사용자 액세스를 관리할 수 있음
스토리지 계정 키 운영자 서비스 역할	Storage Account Key Operator Service Role	스토리지 계정 키 운영자가 스토리지 계정에서 키를 나열하고 다시 생성할 수 있음
읽기 권한자 및 데이터 액세스	Reader and Data Access	모든 항목을 볼 수 있지만, 스토리지 계정 또는 포함된 리소스를 삭제하거나 만들 수는 없고, 스토리지 계정 키에 액세스하면 스토리지 계정에 포함된 모든 데이터에 대한 읽기/쓰기 액세스가 허용됩니다.

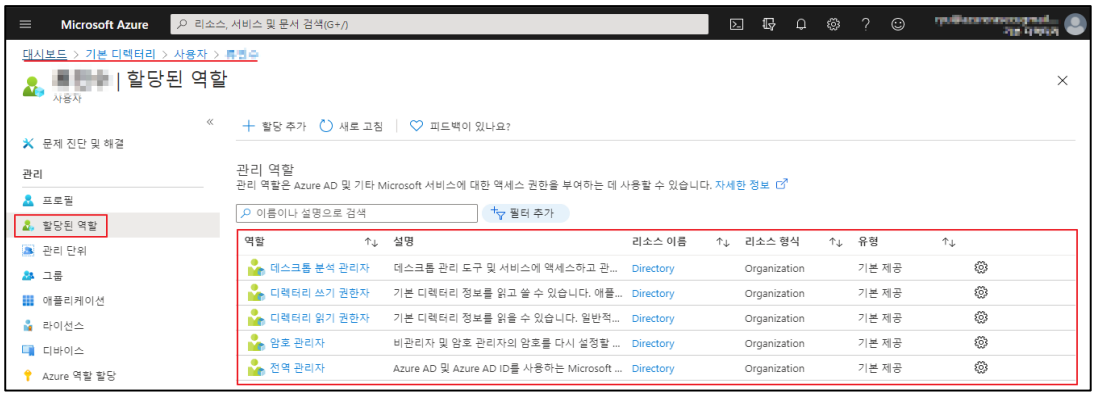
설정 방법

가. Active Directory 사용자 권한 확인

1) Active Directory 사용자 목록 확인



2) Active Directory 사용자의 할당된 역할 확인



나. 사내 클라우드 계정 운영대장 확인

1) 관리자/운영자 접근 계정 운영대장 확인

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							

2) 직무 분류 기준(표) 권한 설정 확인

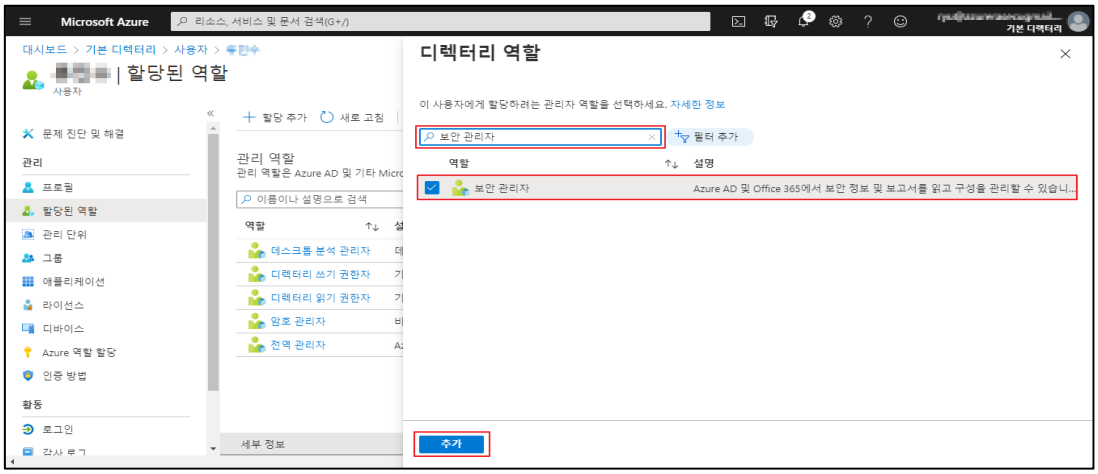
주요 직무 별 사용자 대장				
No.	직무 구분	사용자	부서명	직급
1	Cloud 관리자	XXX	XXX팀	XX
2	Cloud 운영자	XXX	XXX팀	XX
3	Cloud 개발자	XXX	XXX팀	XX
4	정보시스템 관리자	XXX	XXX팀	XX
5	정보시스템 운영자	XXX	XXX팀	XX
6	정보시스템 개발자	XXX	XXX팀	XX
7	정보보호 관리자	XXX	XXX팀	XX
8	정보보호 운영자	XXX	XXX팀	XX
9	정보보호 개발자	XXX	XXX팀	XX
10	비용관리자	XXX	XXX팀	XX
11	비용집행자	XXX	XXX팀	XX

다. Active Directory 사용자 역할 할당하기

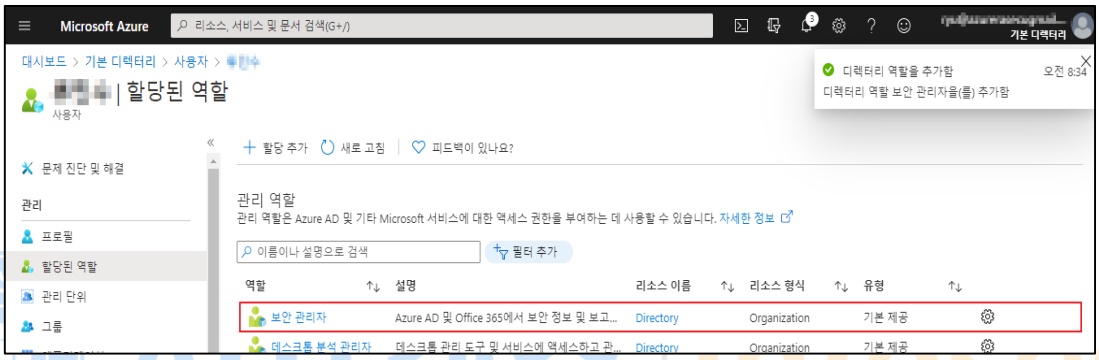
1) Active Directory 사용자 역할 할당 추가

2) Active Directory 사용자 역할 검색

3) Active Directory 사용자 직무 별 역할 부여

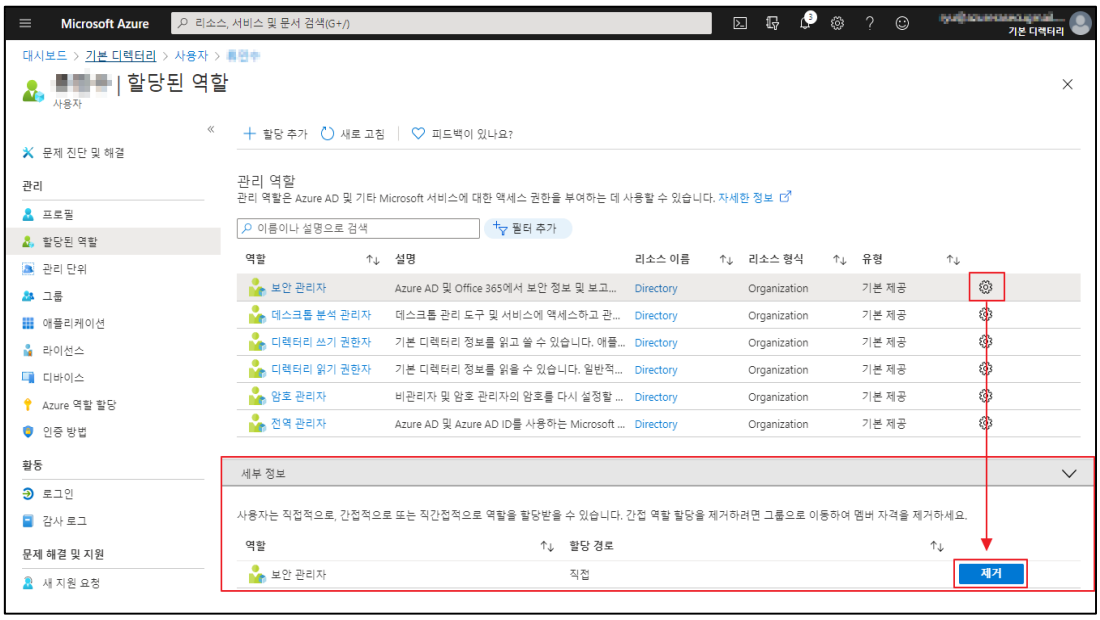


4) Active Directory 사용자에 부여된 역할 확인

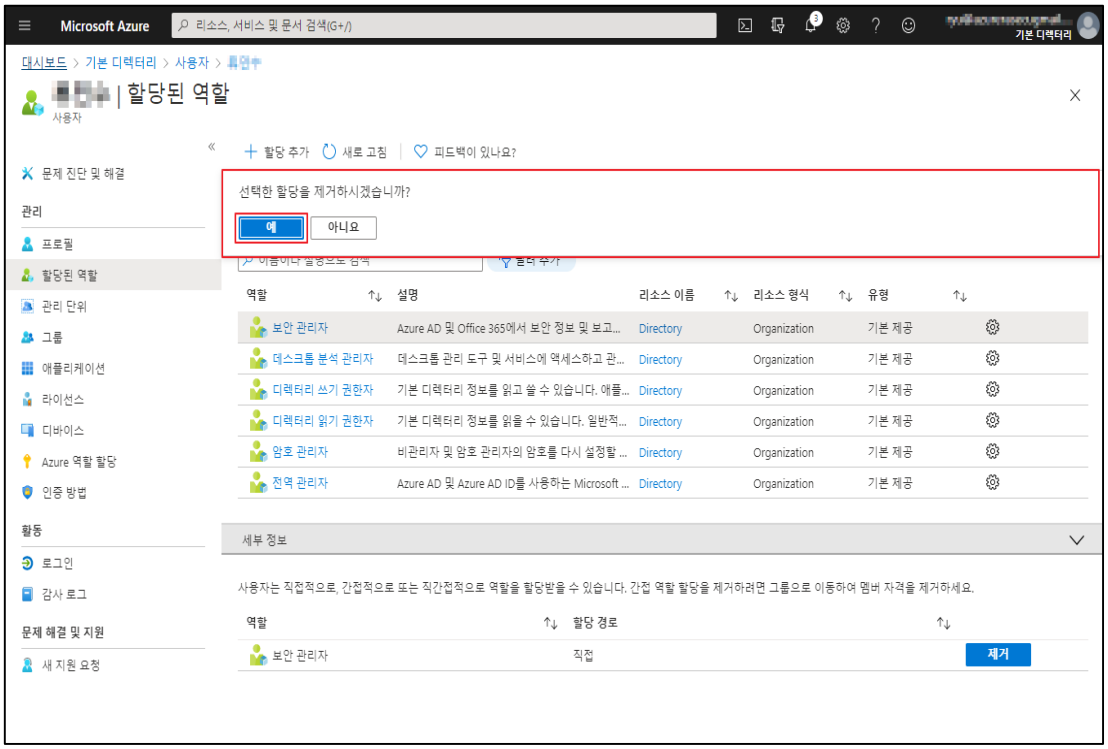


라. Active Directory 사용자 역할 해제하기

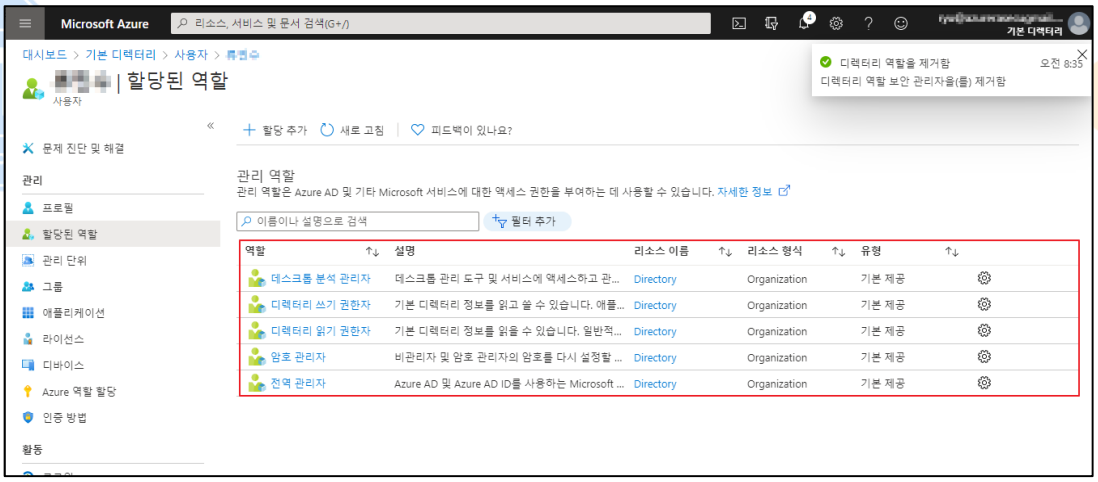
1) Active Directory 사용자 역할 제거



2) Active Directory 사용자 역할 제거 확인



3) Active Directory 사용자 역할이 제거된 목록 확인



진단 기준	**양호기준** : AD 계정(관리자, 소유자, 사용자 등)의 관리 역할이 권한에 맞게 설정되어 있을 경우 **취약기준** : AD 계정(관리자, 소유자, 사용자 등)의 관리 역할이 권한에 맞게 설정되어 있지 않을 경우
비고	

1.7 Key Vault 액세스 정책

분류	권한관리	**중요도**	상
항목명	Key Vault 액세스 정책		

항목 설명

클라우드 응용 프로그램 및 서비스를 보호하기 위한 암호화 키, 비밀 및 인증서를 보호하고 안전하게 액세스 하기 위해 Key Vault 가 사용됩니다.

※ Key Vault 사용 (예시)

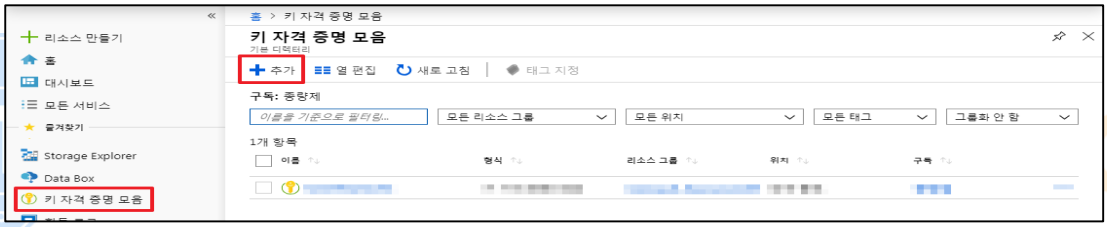
종류	내용
비밀 관리	토큰, 암호, 인증서, API 키 및 기타 비밀을 액세스를 제어
키 관리	페이지를 만들고 데이터를 암호화 하는 키를 제어
인증서 관리	내부 리소스에 대한 공용 및 개인 SSL/TLS 인증서를 배포
HSM 에서 지원하는 암호저장	소프트웨어 또는 FIPS 140-2 Level 2 HSM 키와 암호를 보호하기 위한 유효성을 검사

또한 Key Vault 를 사용하면 하드웨어 보안모듈(Hsm)로 보호 된 키를 사용하여 인증 키, 저장소 계정 키, 데이터 암호화 키, pfx 파일 및 암호를 암호화할 수 있어, Key Vault 에 대해 관리 권한을 갖는 사용자 또는 그룹만 접근할 수 있도록 액세스 정책을 수립해야 합니다.

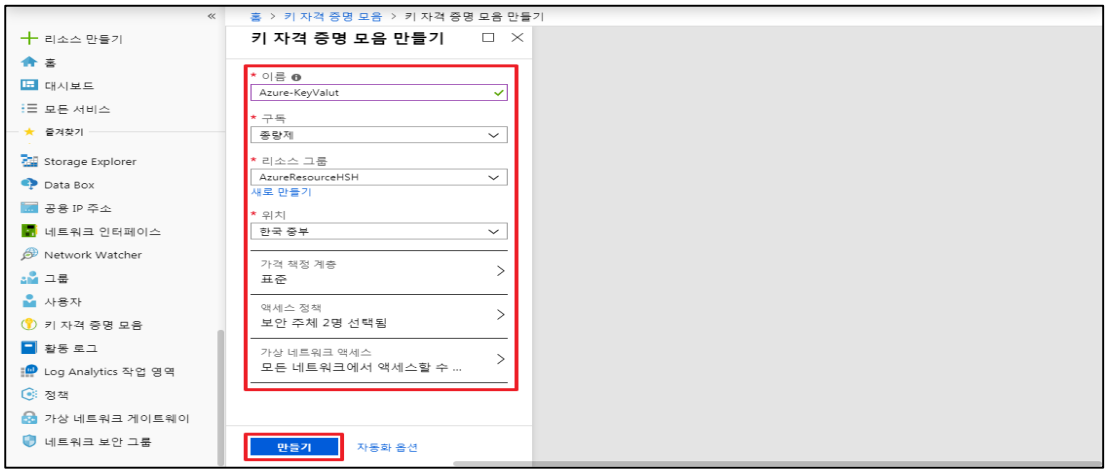
설정 방법

가. 키 자격 증명 모음(Key Vault) 생성 방법

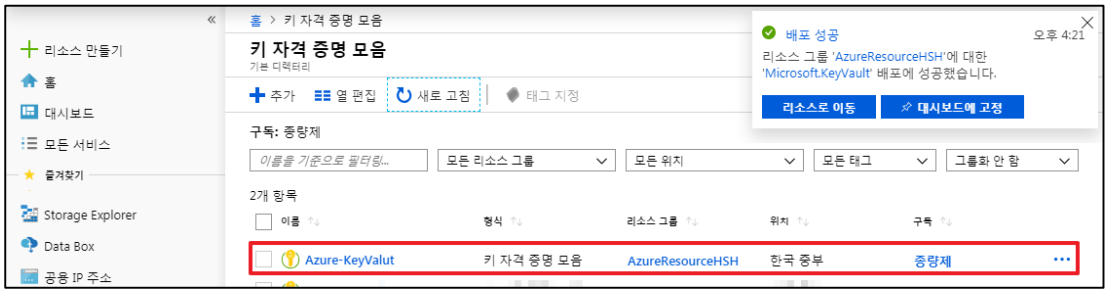
1) 키 자격 증명 모음(Key Vault) 메뉴 내 추가 버튼 클릭



2) 생성할 키 자격 증명 옵션 설정

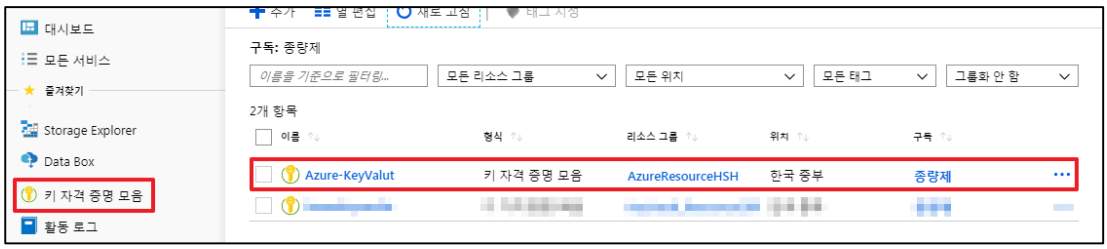


3) 키 자격 증명 모음(Key Vault) 목록 내 정상 생성 여부 확인

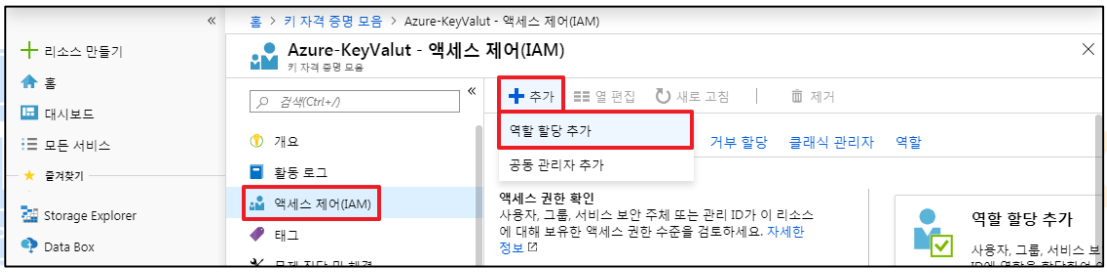


나. 키 자격 증명 모음(Key Vault) 내 액세스 제어(IAM) 설정 방법

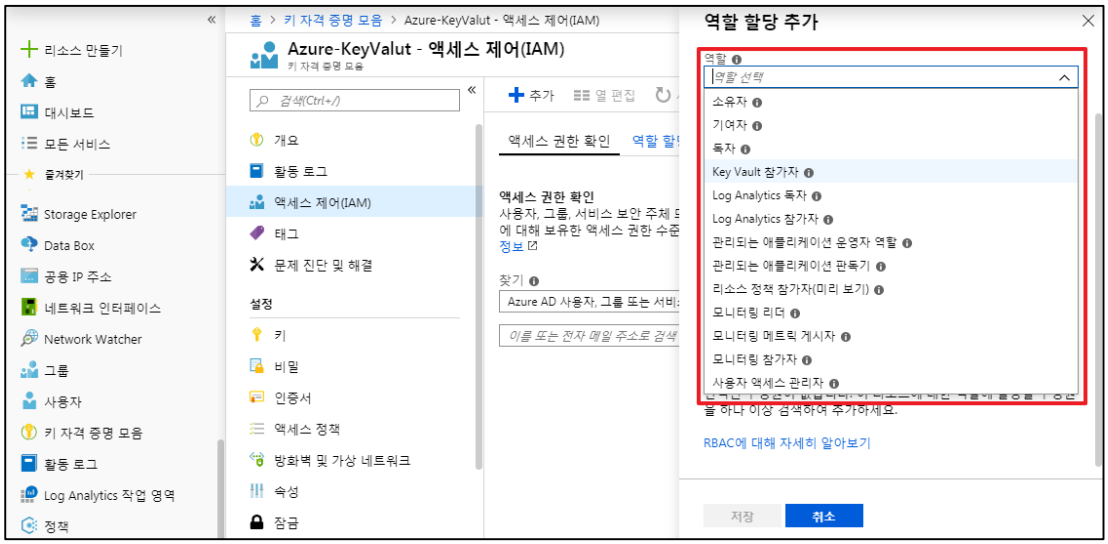
1) 액세스 제어를 설정할 키 자격 증명 모음(Key Vault) 선택



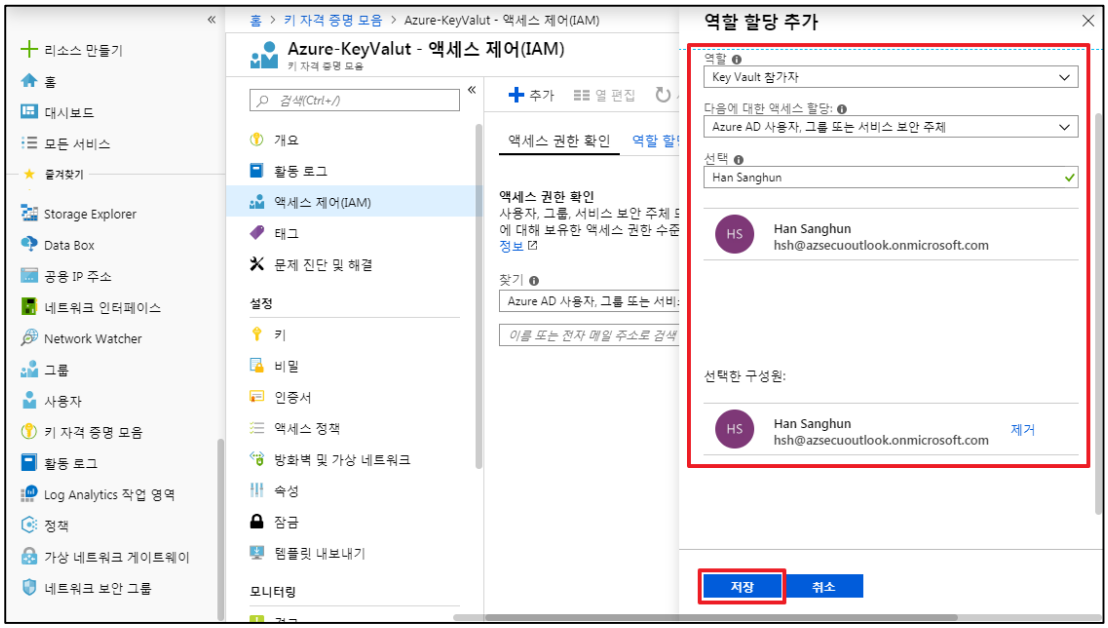
2) 내 액세스 제어(IAM) 선택 후 역할 할당 추가 버튼 클릭



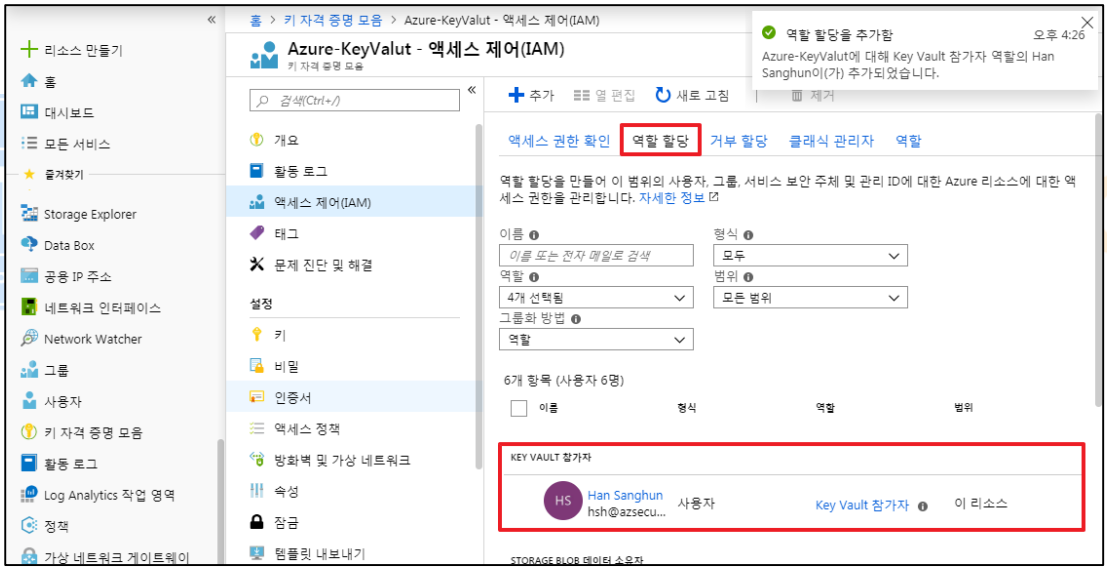
3) 추가할 역할/권한 선택



4) 역할/권한을 설정할 사용자 선택

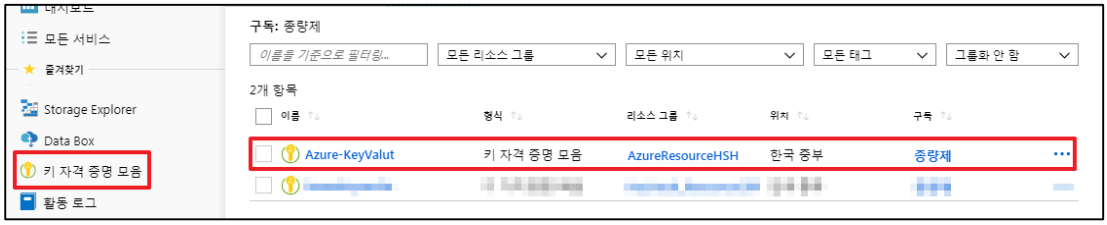


5) 액세스 제어(IAM) 메뉴 내 역할 할당 메뉴에서 설정된 역할/권한 및 계정 확인

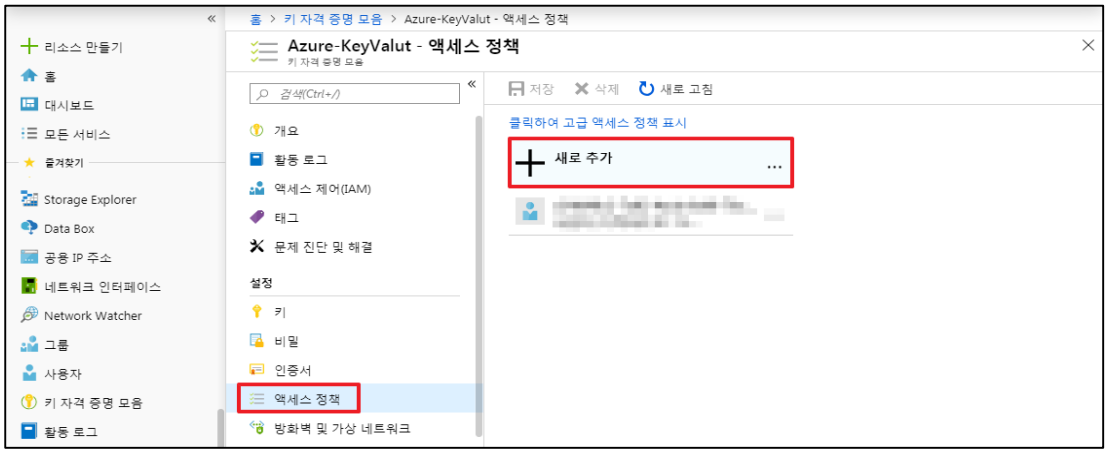


다. 키 자격 증명 모음(Key Vault) 내 액세스 정책(보안주체 및 권한) 설정 방법

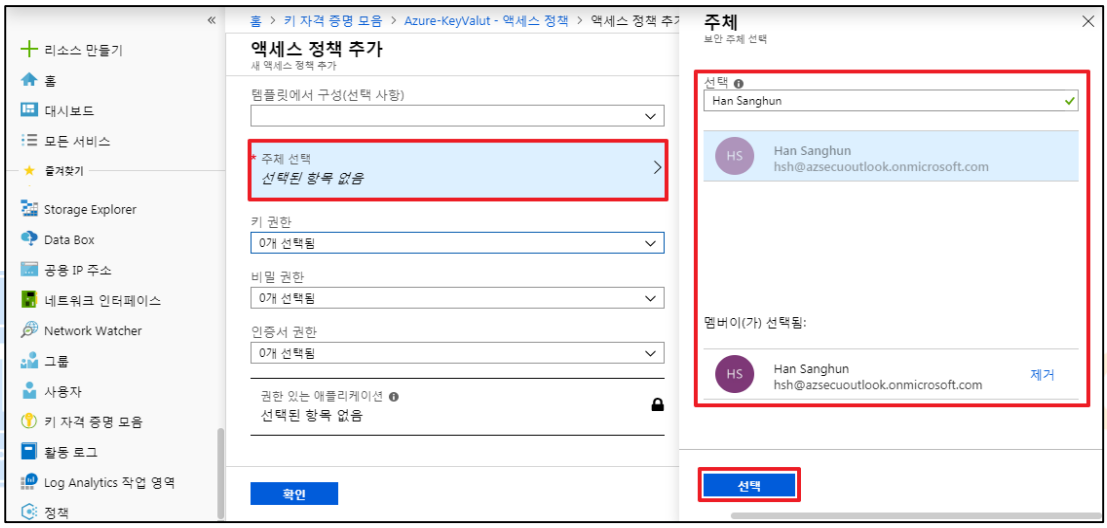
1) 액세스 정책을 설정할 키 자격 증명 모음(Key Vault) 선택



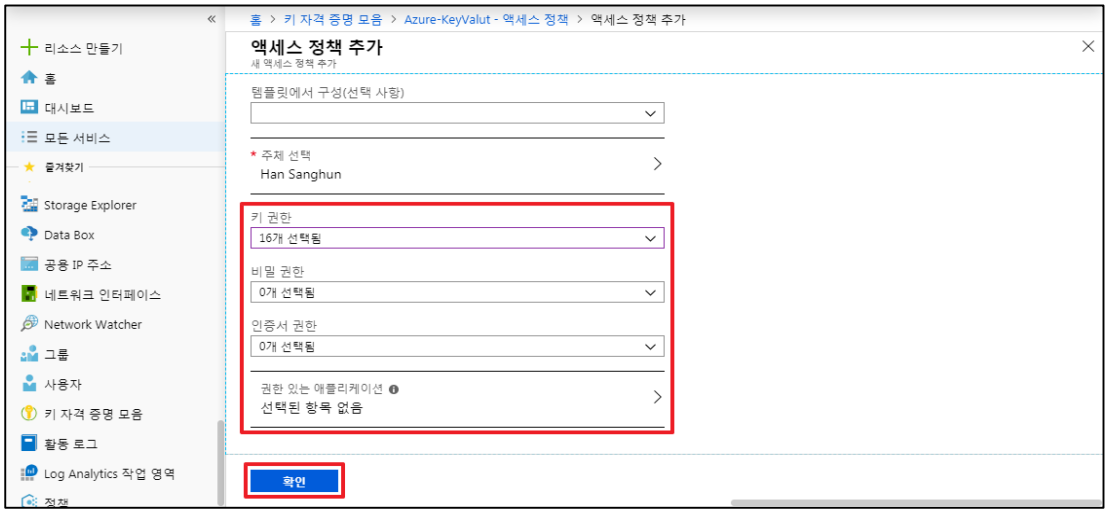
2) 내 액세스 정책 선택 후 역할 새로 추가 버튼 클릭



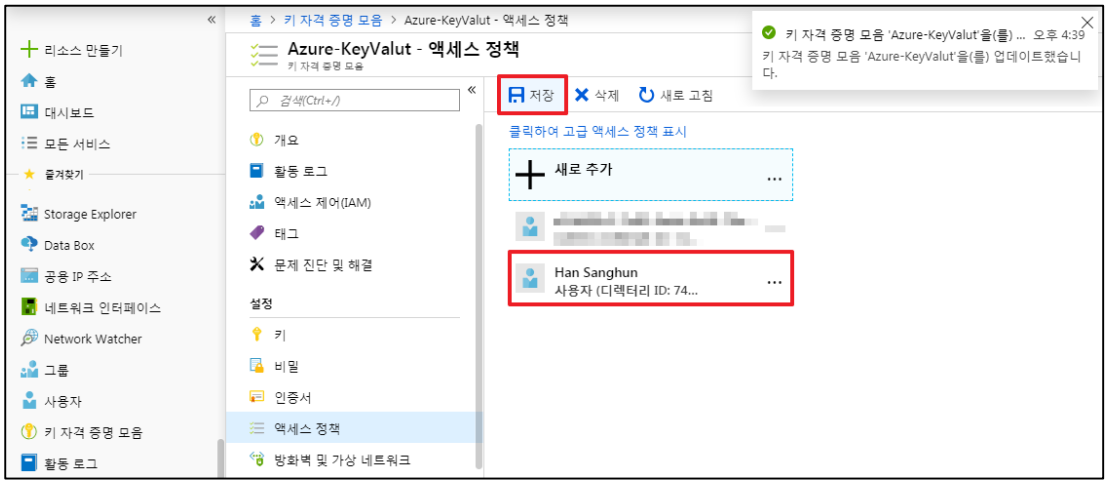
3) 정책을 설정할 사용자(보안주체) 선택



4) 선택된 사용자의 키/비밀/인증서/애플리케이션 권한 설정



5) 정상 설정 여부 확인 및 저장

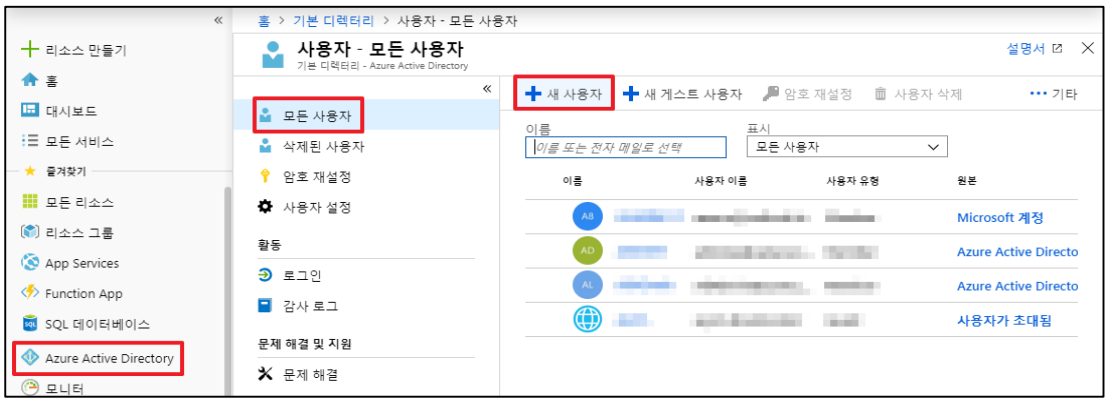
	
진단 기준	**양호기준** : 키/비밀/인증서 권한 관리정책에 맞게 Key Vault가 발급되어 사용하고 있을 경우 **취약기준** : 키/비밀/인증서 권한 관리정책에 맞게 Key Vault가 발급되어 사용하고 있지 않을 경우
비고	

2. 계정관리

2.1 AD 사용자 계정 최고 권한 관리

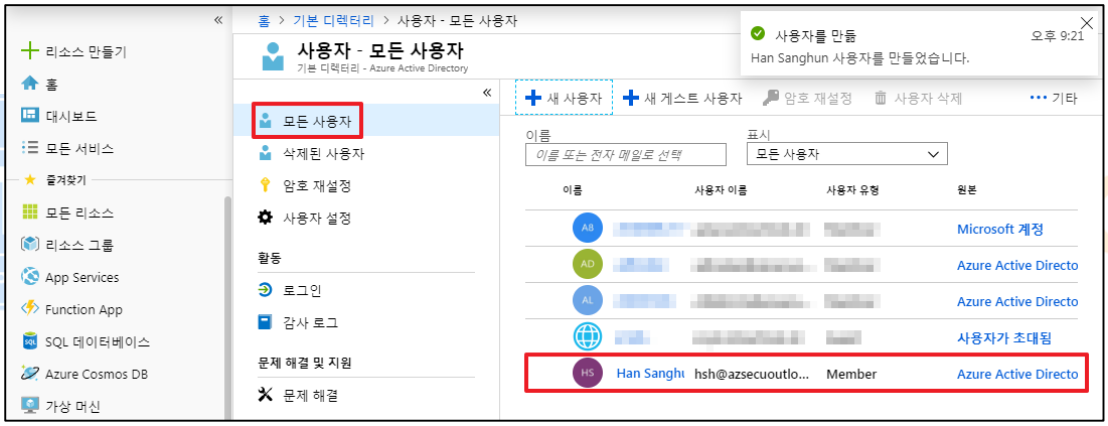
<table>
<tr><td>분류</td><td>계정관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">AD 사용자 계정 최고 권한 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Azure AD를 사용하는 사용자의 효율적인 관리를 위해 프로필을 구성할 수 있으며, 네이밍룰 등을 적용하여 사용자의 권한, 역할 등을 표기하여 관리할 수 있습니다. 또한 디렉터리 역할 설정을 통해 사용자의 관리역할 부여가 가능합니다.

※ 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 관리역할을 보유</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">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
 

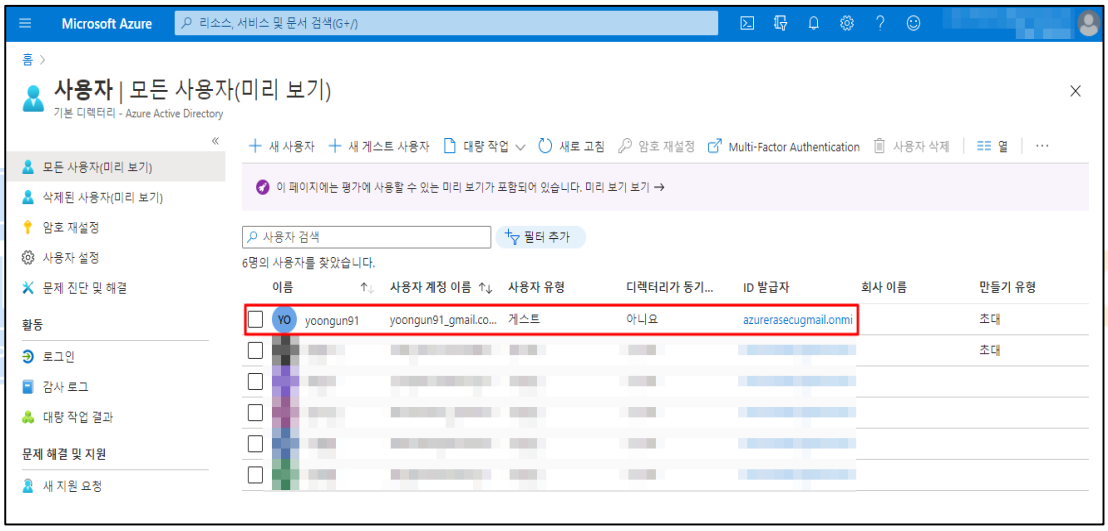
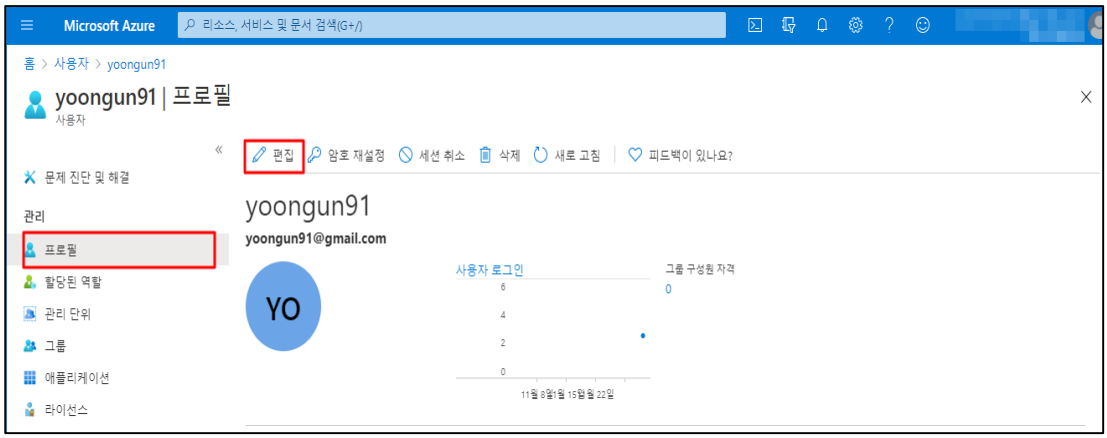
3) 사용자 정보 입력 및 디렉터리 역할 선택 시 전역/제한된 관리자 선택</td></tr>
</table>

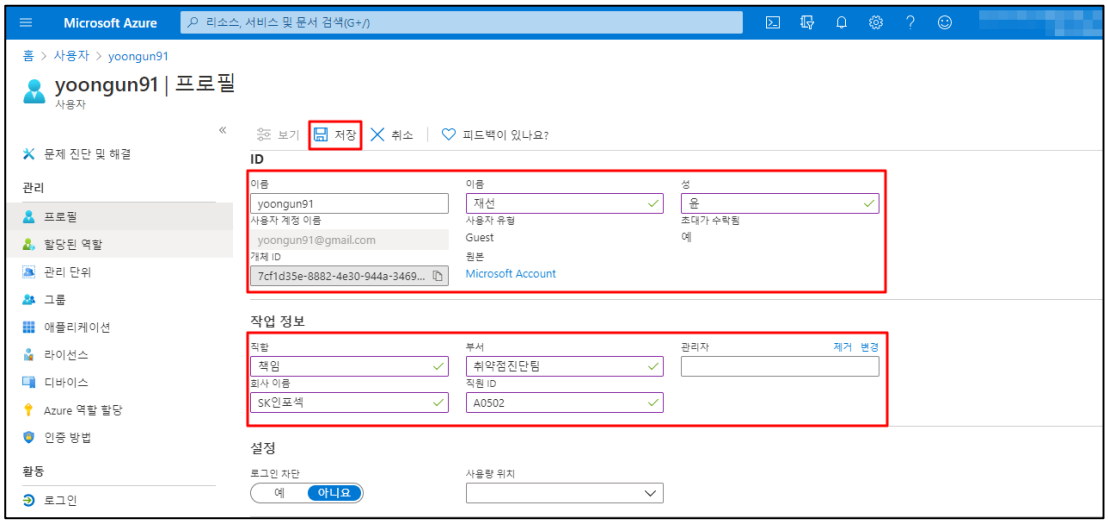
4) 모든 사용자 목록 내 전역/제한된 관리자 생성 여부 확인



진단 기준	**양호기준** : 사용자 계정에 '전역 관리자' 및 '제한된 관리자' 역할이 부여되어 있지 않을 경우 **취약기준** : 사용자 계정에 '전역 관리자' 및 '제한된 관리자' 역할이 부여되어 있을 경우
비고	

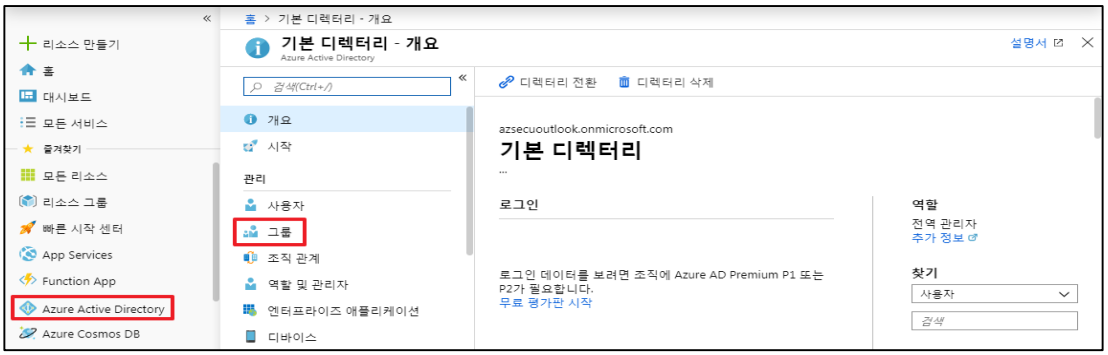
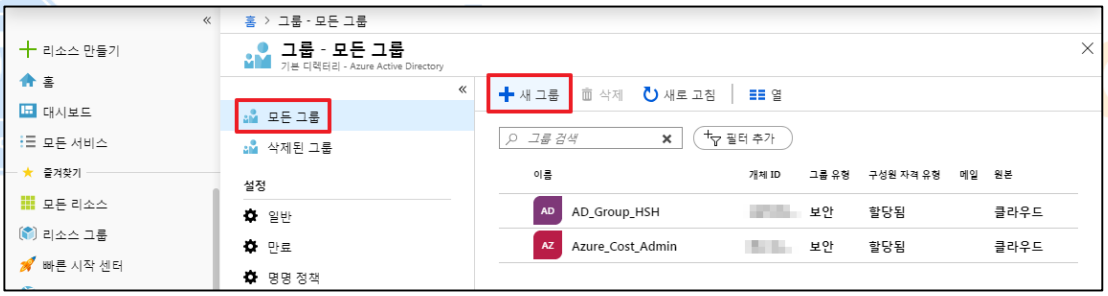
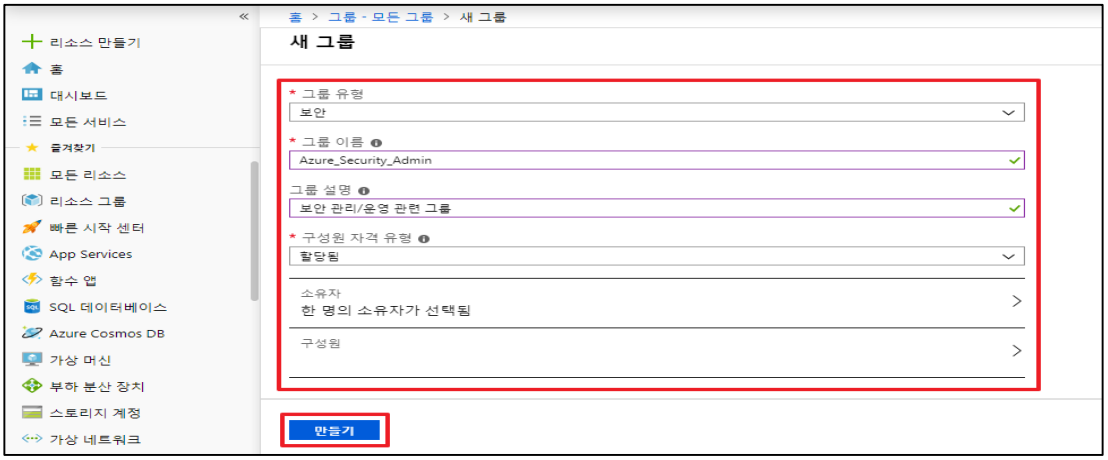
2.2 AD User 프로필 및 디렉터리 식별 관리

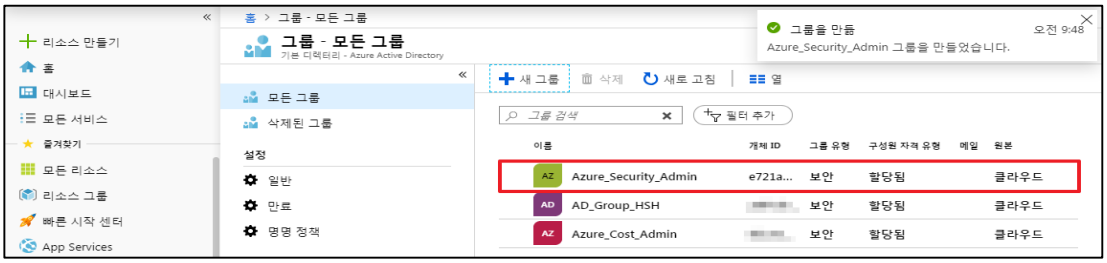
분류	계정관리	중요도	중
항목명	AD User 프로필 및 디렉터리 식별 관리		
항목 설명	생성된 Active Directory 사용자에 대한 정보를 프로필 가능을 통해 추가, 수정할 수 있습니다. 사용자 계정에 대한 프로필 정보는 서비스 사용에 대한 식별/감사/추적 등을 명확하게 할 수 있기 때문에 정확한 정보를 기입하는 것이 필요합니다. **※ 프로필 작성 필수 항목** ID - 계정 사용자 성명 기입 작업 정보 - 부서/직함 기입, 관리자 선택 (게스트 계정일 경우 필수) 연락처 정보 - 메일 주소 기입		
설정 방법	**가. 사용자 프로필 정보 확인 및 설정 방법** 1) Active Directory의 사용자 리스트 내 개별 사용자 클릭  2) 사용자 프로필 메뉴의 편집 버튼 클릭  3) 프로필 정보 확인 및 수정 후 저장 클릭		

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: 프로필 정보를 네이밍룰 등을 적용하여 사용자 역할 등을 식별할 수 있도록 표기하여 사용하고 있을 경우

취약기준
: 프로필 정보를 네이밍룰 등을 적용하여 사용자 역할 등을 식별할 수 있도록 표기하여 사용하고 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

2.3 AD 그룹 구성원 및 소유자 관리

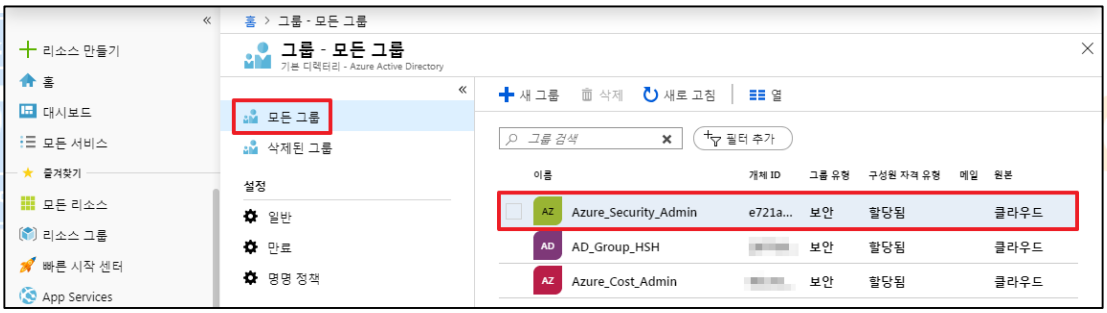
분류	계정관리	중요도	중
항목명	AD 그룹 구성원 및 소유자 관리		
항목 설명	Azure AD를 사용 시 그룹을 통해 권한을 할당하거나 리소스에 대한 액세스 권한을 부여할 수 있으며, 해당 그룹 구성원인 사용자는 그룹의 액세스 권한을 상속받게 됩니다. 또한 그룹은 소유자를 지정하여 그룹 및 그룹 구성원을 관리할 수 있습니다.		
설정 방법	**가. Azure Active Directory(Azure AD) 그룹 생성 방법** 1) Azure AD 메뉴 내 그룹 기능 선택  2) 그룹메뉴 내 새 그룹 버튼 클릭  3) 그룹 관련 내용 설정 및 만들기(소유자/구성원의 경우 미설정 시 추후 별도 추가 가능)  4) 모든 그룹 목록 내 정상 생성 여부 확인		



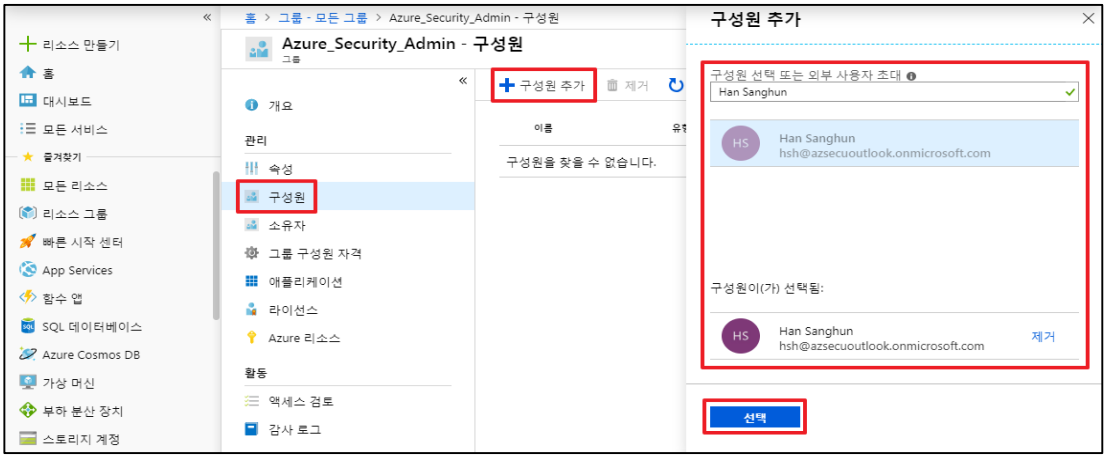
나. Azure Active Directory(Azure AD) 그룹 내 역할별 소유자/구성원 설정 방법

1) Azure AD 메뉴 내 그룹 기능 선택

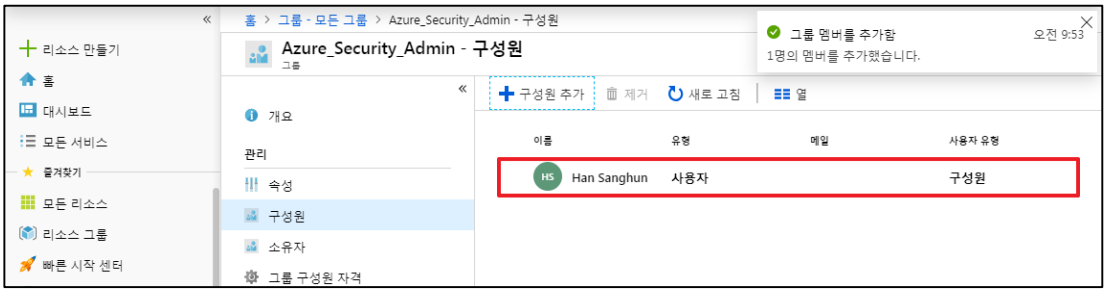
2) 소유자/구성원을 추가할 그룹 선택



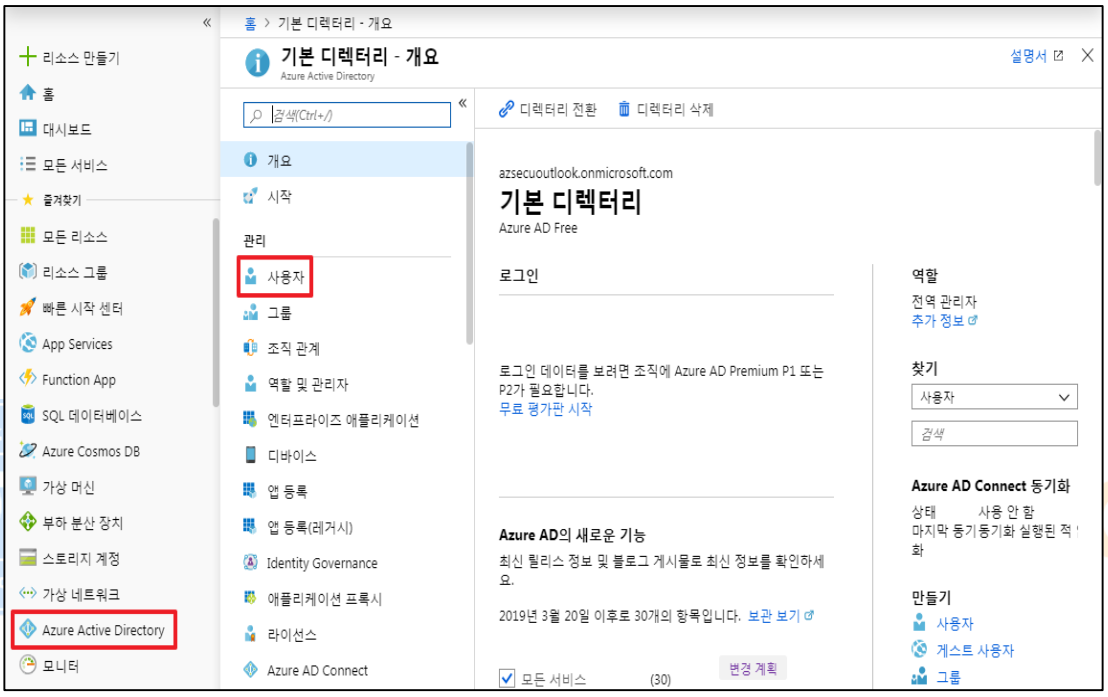
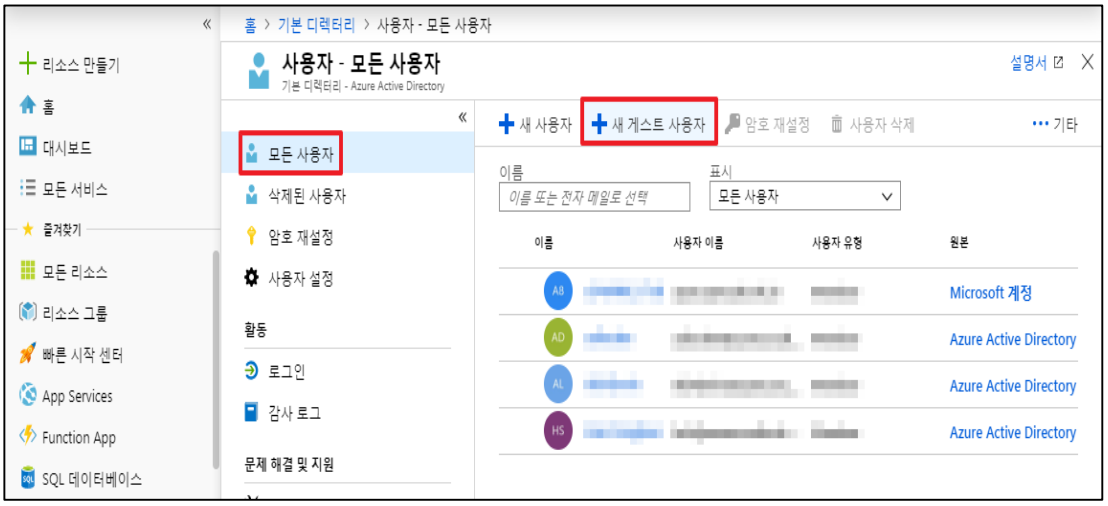
3) 구성원 기능 선택 후 구성원 추가 버튼클릭 및 추가할 구성원 검색(소유자 설정방식 동일)



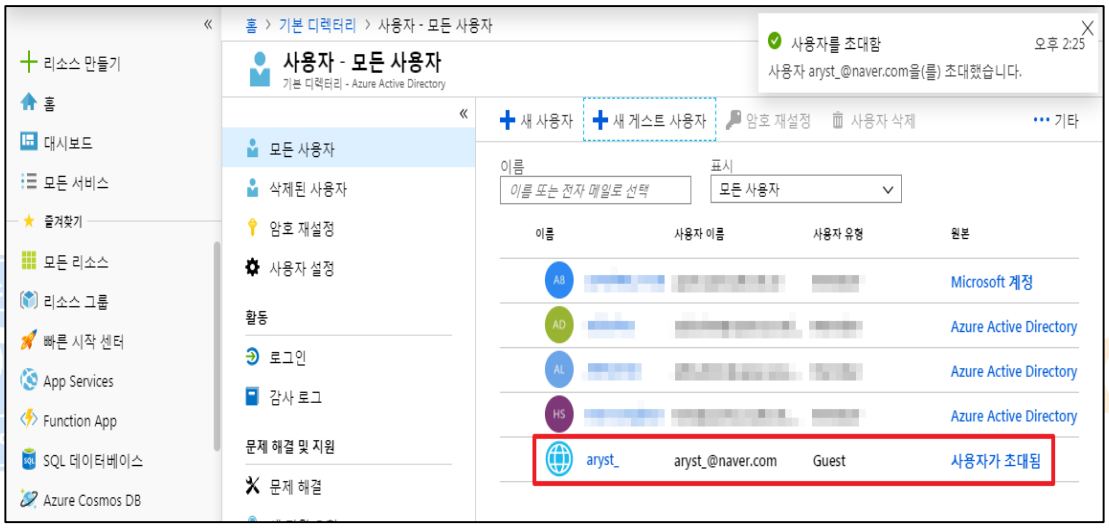
4) 구성원 목록 내 정상 생성 여부 확인

	
진단 기준	**양호기준** : 그룹 내 역할에 알맞은 사용자가 소유자로 설정 되어 있고, 필요한 구성원만 포함되어 있을 경우 **취약기준** : 그룹 내 역할에 알맞은 사용자가 소유자로 설정 되어 있지 않고, 불필요한 구성원이 포함되어 있을 경우
비고	

2.4 AD 게스트 사용자

분류	계정관리	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 새 게스트 사용자 버튼 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

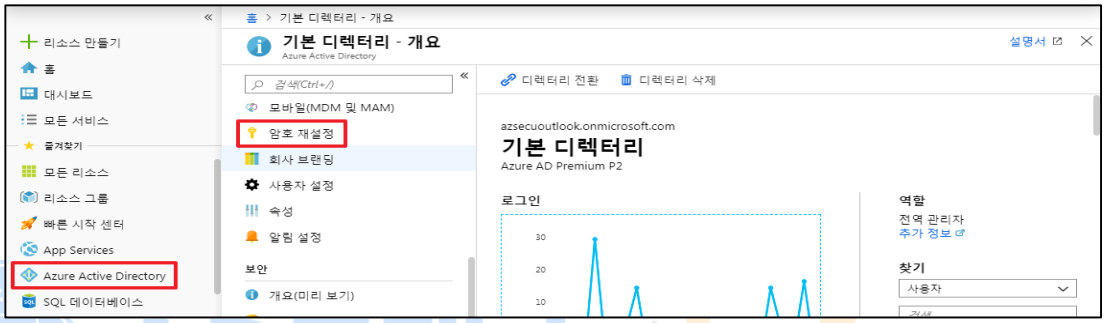
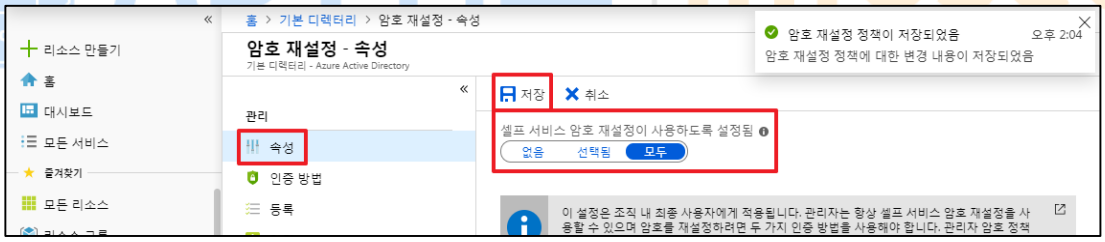
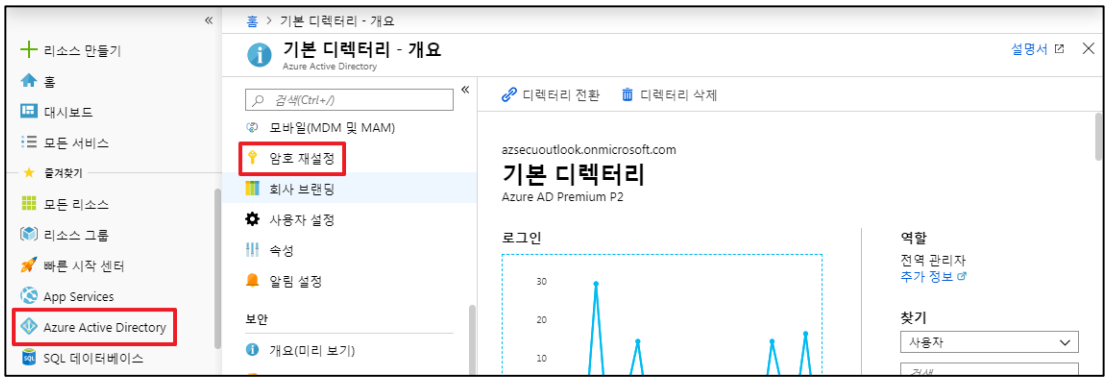
<table>
<tr>
<td></td>
<td>

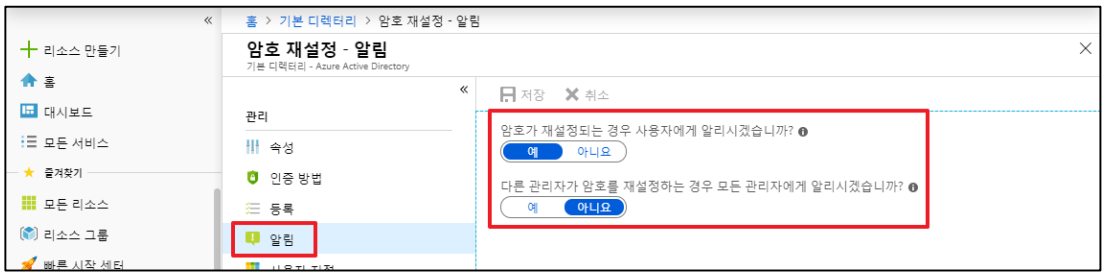

7) Azure 정상 로그인 여부 확인


</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 게스트 사용자 계정(사용 만료 된 불필요한 계정 포함)이 존재하지 않고, 목적에 맞는 권한을 사용하고 있을 경우

취약기준
: 게스트 사용자 계정(사용 만료 된 불필요한 계정 포함)을 존재 하고, 목적에 맞지 않는 권한을 사용하고 있을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

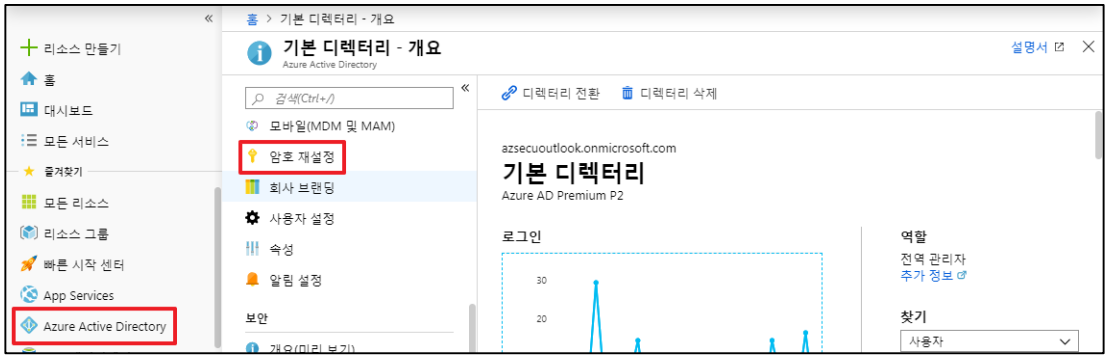
2.5 AD 암호 재설정 관리

분류	계정관리	중요도	하
항목명	AD 암호 재설정 관리		
항목 설명	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 있으며 암호를 잊어버릴 때마다 기술지원팀과 통화 등을 진행할 필요가 없어 즉각적인 처리가 가능한비다. **※ 셀프 서비스 암호 재설정 기능은 프리미엄 구독을 신청한 경우에 사용이 가능함.**		
설정 방법	**가. 셀프 암호 재설정 기능 설정 방법** 1) Azure Active Directory 메뉴 내 암호 재설정 기능 선택  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		

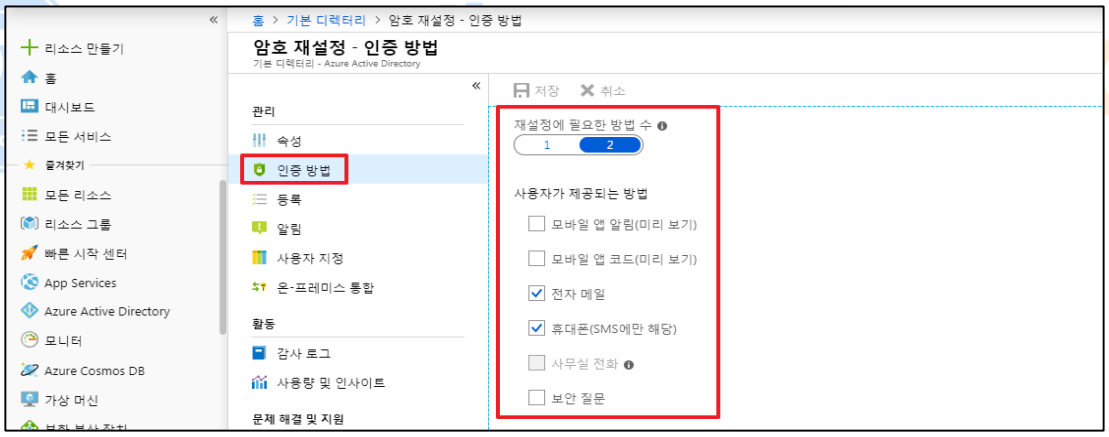


다. 인증 방법 설정 방법

1) Azure Active Directory 메뉴 내 암호 재설정 기능 선택



2) 인증 방법 메뉴 내 인증 방법 설정



진단 기준	**양호기준** : 셀프 서비스 암호 재설정을 사용하도록 설정되어 있을 경우 **취약기준** : 셀프 서비스 암호 재설정을 사용하도록 설정되어 있지 않을 경우
비고	

2.6 MFA (Multi-Factor Authentication) 설정

분류	계정관리	중요도	상
항목명	MFA (Multi-Factor Authentication) 설정		

항목 설명

MFA(2차 인증방식)의 보안은 계층화된 접근 방식을 기반으로 합니다. 공격자는 사용자의 암호를 알게 된 경우에도 추가 인증 메서드가 없다면 계정을 손상시키거나 액세스하기 더욱 어렵습니다. 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

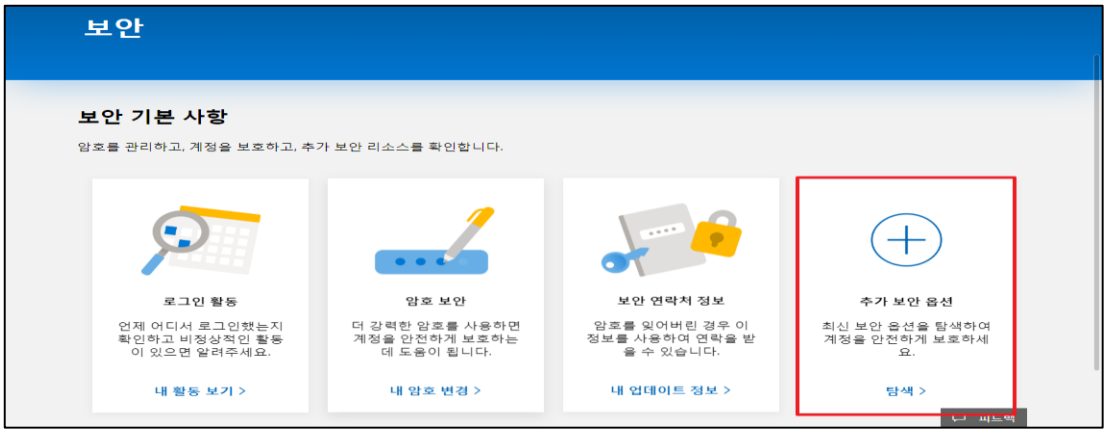
기능	설명
계정잠금	연이어 거부된 인증 시도가 너무 많은 경우 Multi-Factor Authentication 서비스에서 계정을 일시적으로 잠급니다. 이 기능은 인증을 위해 PIN을 입력하는 사용자에게만 적용됩니다. **※ 계정잠금 기능은 프리미엄 구독을 신청한 경우에 사용이 가능함.**
사용자 차단 / 차단 해제	특정 사용자가 Multi-factor Authentication 요청을 받을 수 없도록 차단 하는 데 사용 합니다. 차단된 사용자에 대한 모든 인증 시도가 자동으로 거부됩니다. 사용자는 차단된 시간 이후 90일 동안 차단된 상태로 유지됩니다.
사기 행위 경고	사용자가 사기성 확인 요청을 보고서 수와 관련 된 설정 구성
알림	MFA 서버의 이벤트 알림이 가능하도록 설정합니다.
OAUTH 토큰	클라우드 기반 Azure MFA 환경에 사용되어 사용자의 OAUTH 토큰을 관리합니다.
전화 통화 설정	클라우드 및 온-프레미스 환경의 인사말 및 전화 통화 관련 설정을 구성합

설정 방법

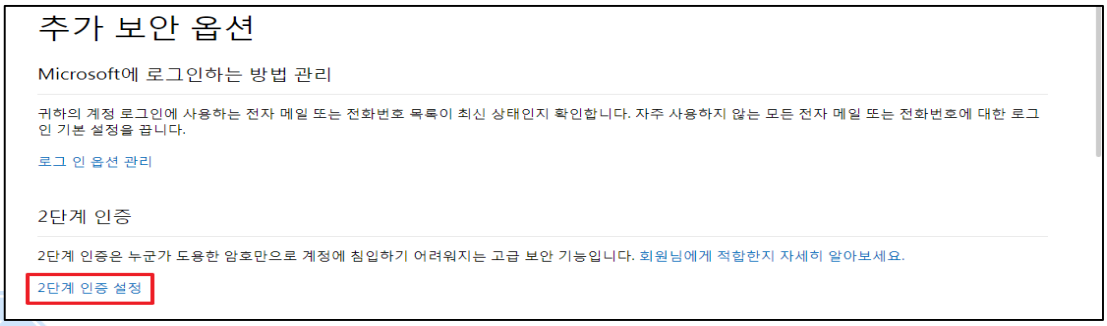
가. MFA 설정 방법 (MS 계정)

1) MS 계정 페이지 내 보안 정보 업데이트 메뉴 클릭

2) 보안 기본 사항 메뉴 내 추가 보안 옵션 메뉴 클릭

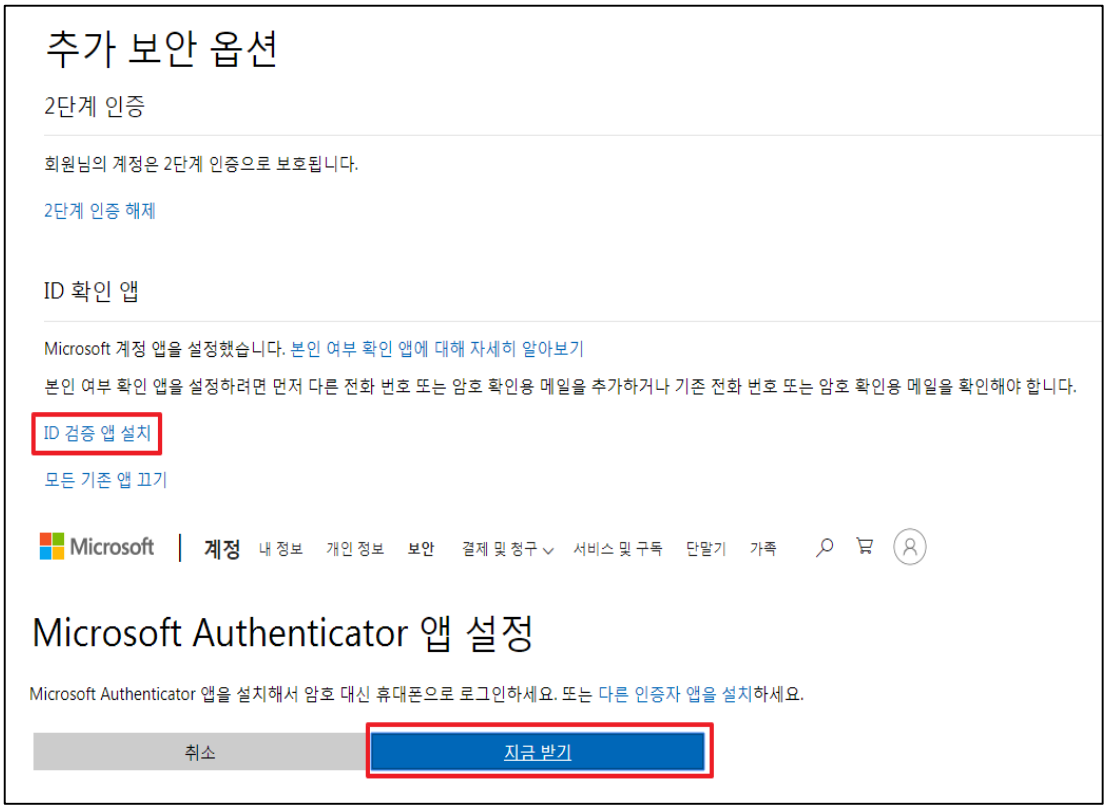


3) 2단계 인증 메뉴 내 2단계 인증 설정 클릭

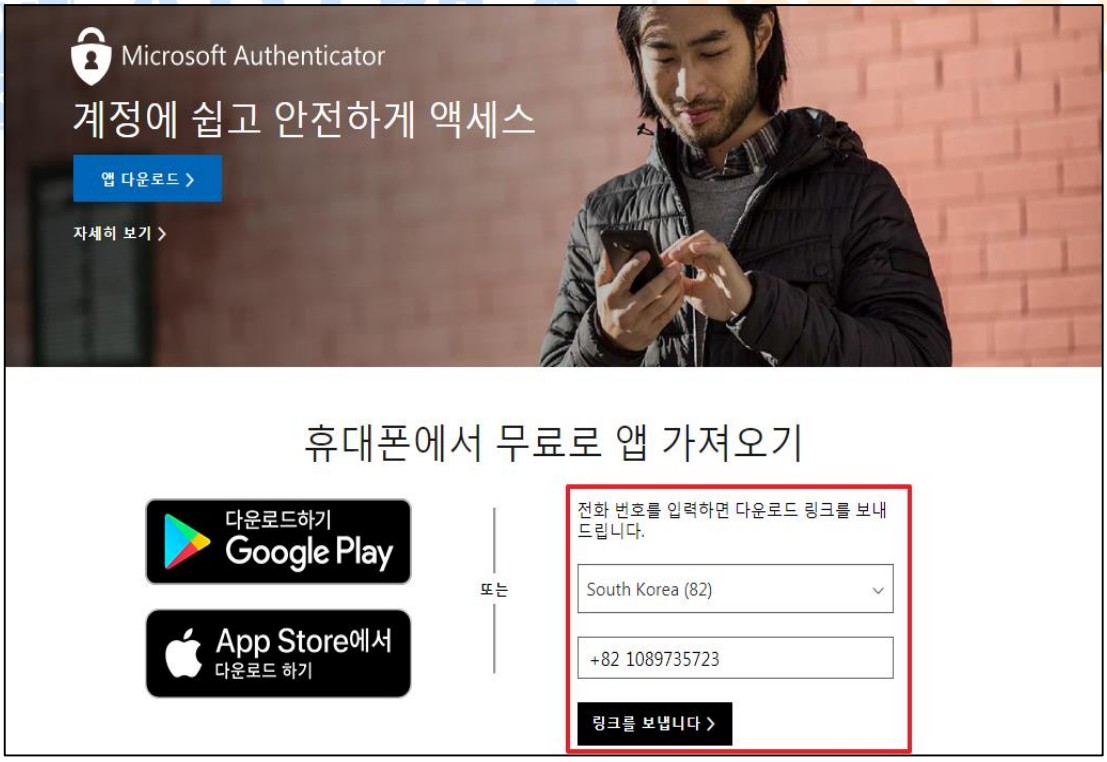


4) 인증 설정 내용 확인 및 마침 (2단계 인증 사용 설정 완료)

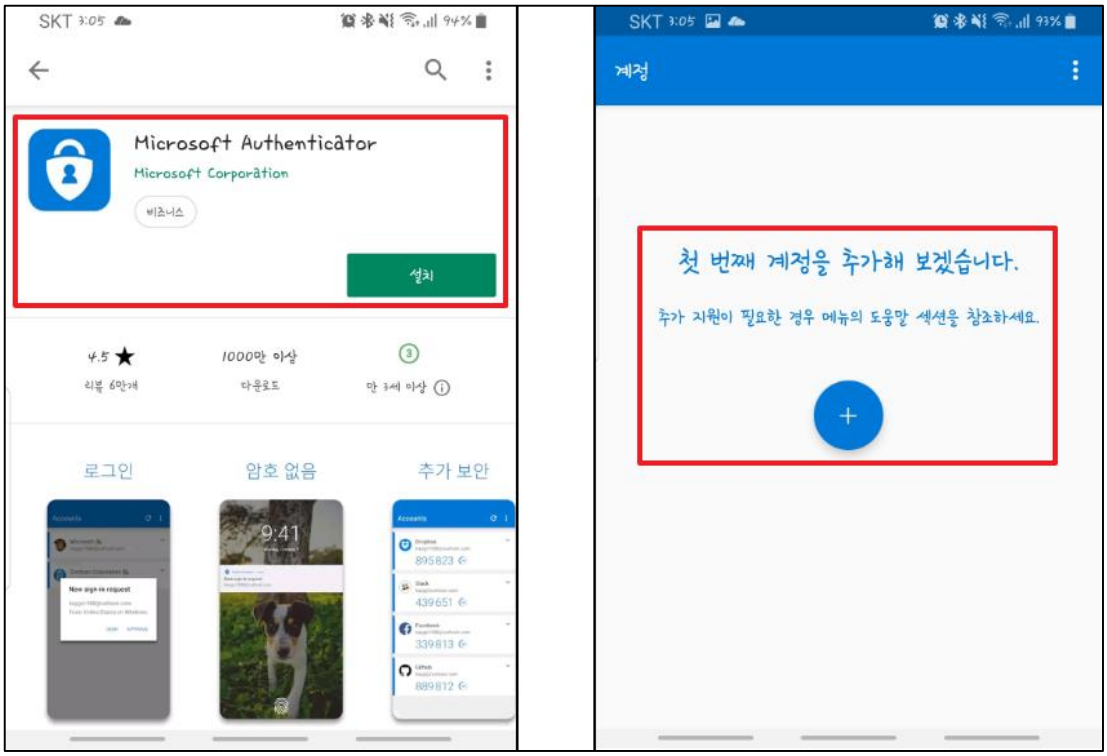
5) ID 확인 앱 메뉴 내 ID 검증 앱 설치 및 지금 받기 클릭



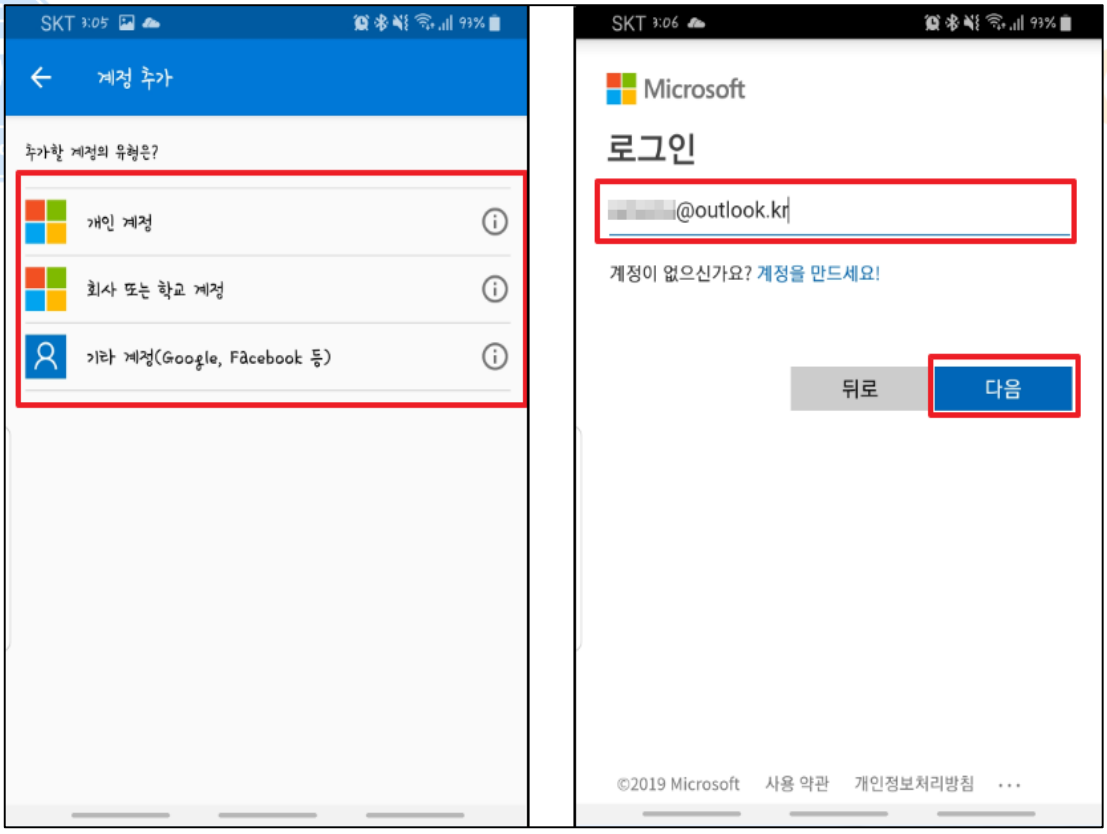
6) 앱 설치 링크를 전달받을 연락처 작성 및 링크 보내기



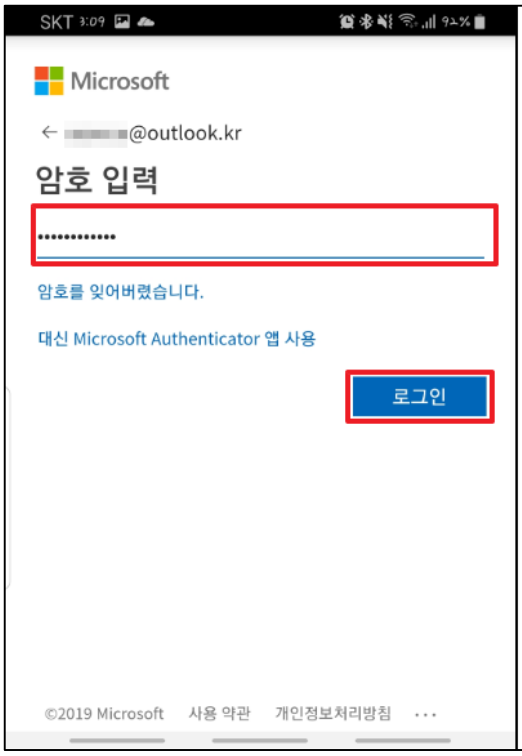
7) MS Authenticator 앱 설치 및 실행 후 계정 추가 (링크 전송 실패 시 직접 검색 및 설치 가능)

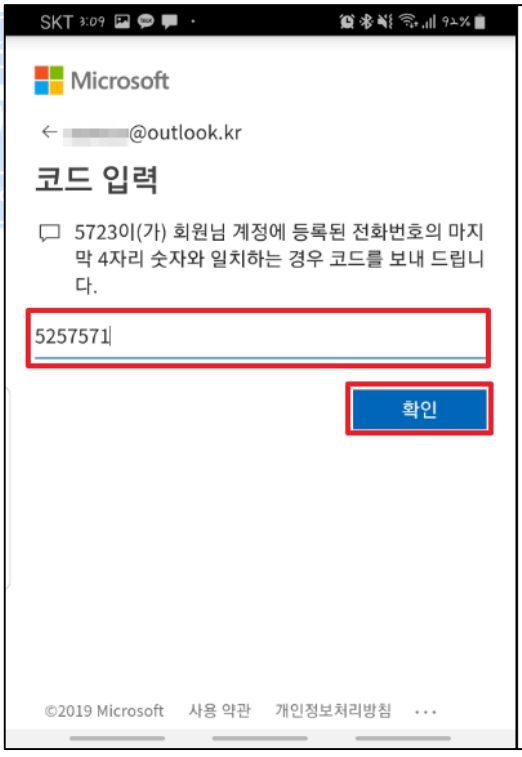


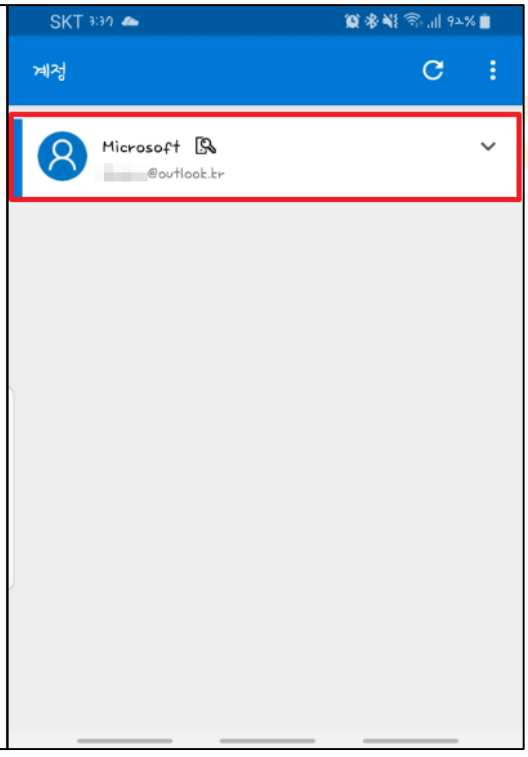
8) MS 계정 로그인 진행

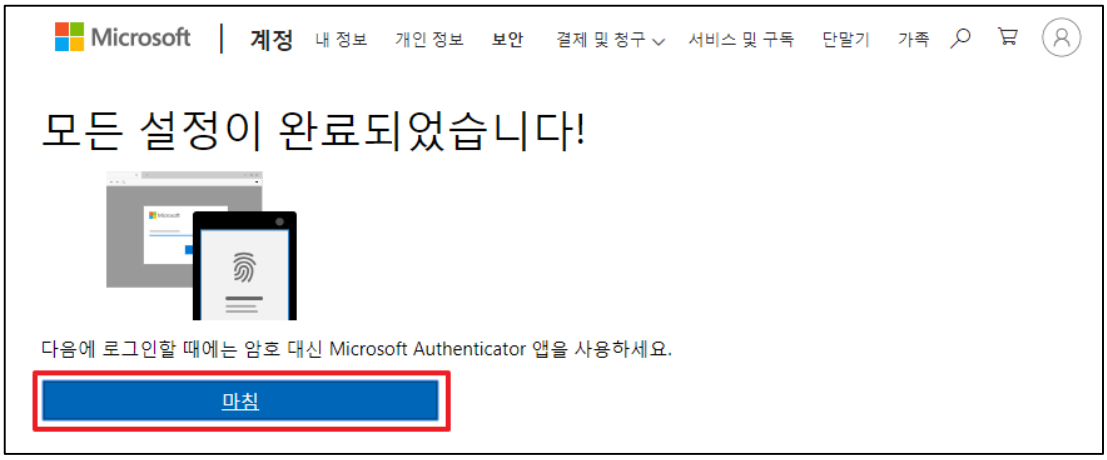


9) 로그인에 필요한 본인 인증 진행 및 설정 완료

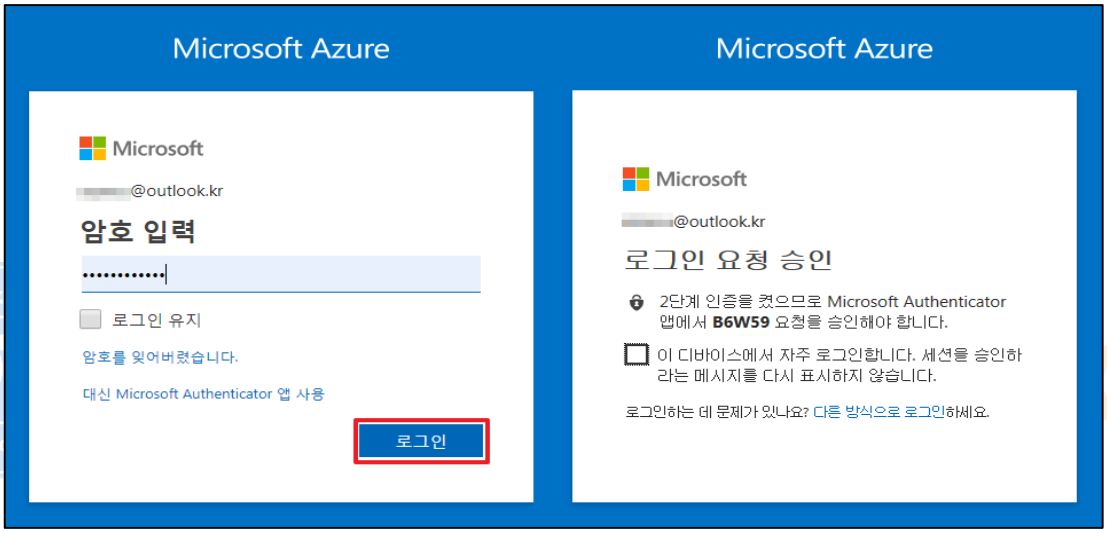




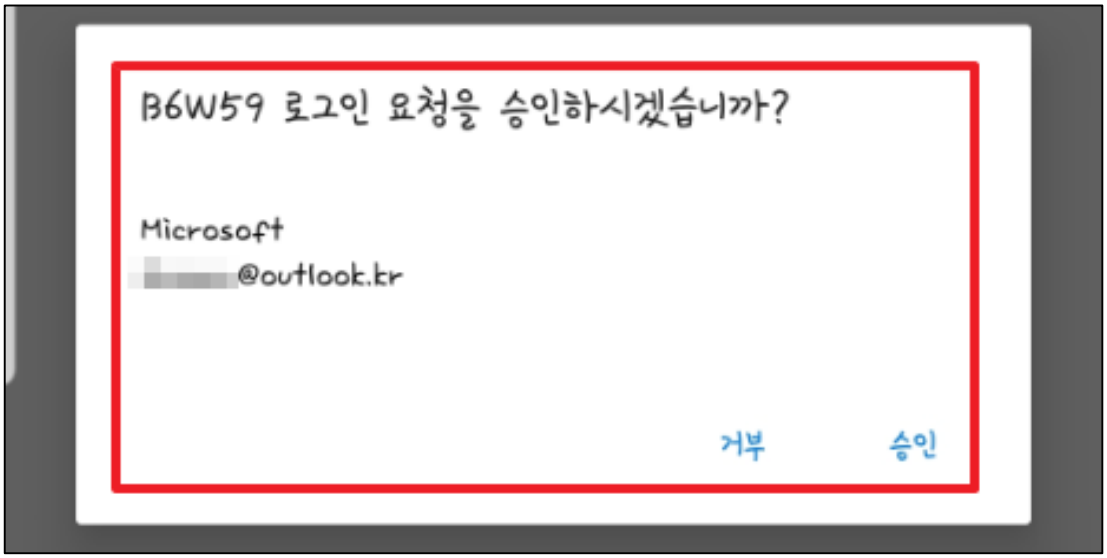




10) MS 계정으로 Azure 로그인 진행

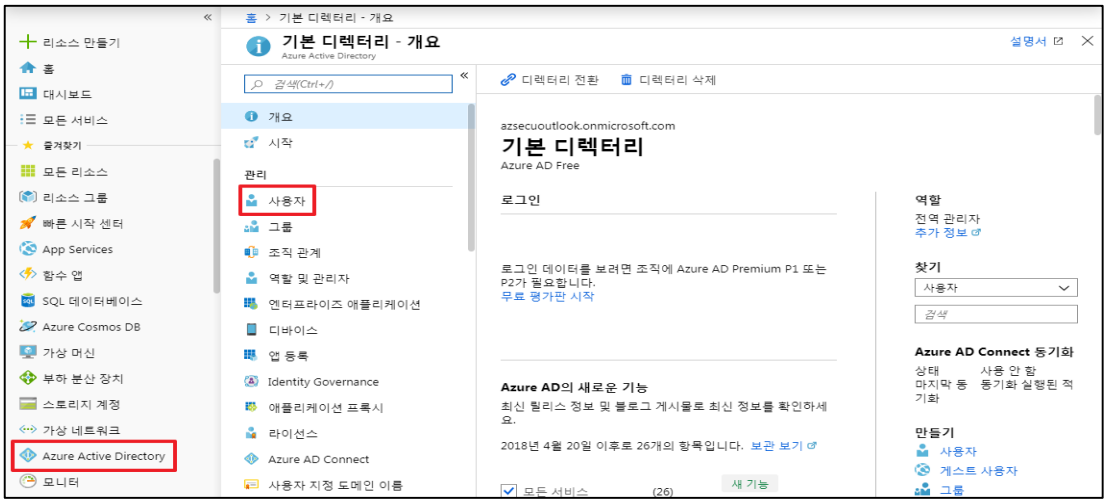


11) MS Authenticator 앱 내 로그인 요청 승인



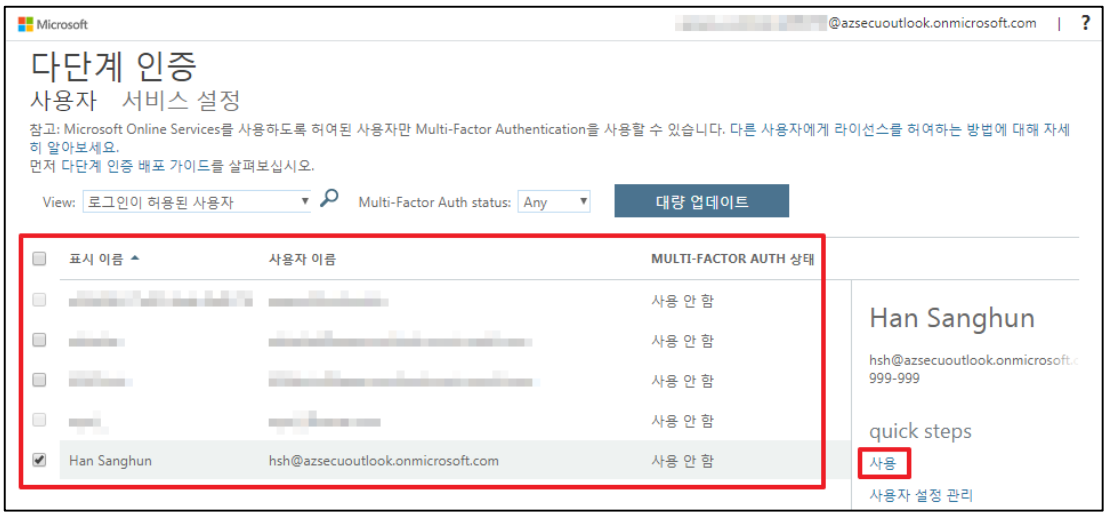
나. MFA 설정 방법 (Azure Active Directory 계정)

1) Azure Active Directory 메뉴 내 사용자 기능 선택

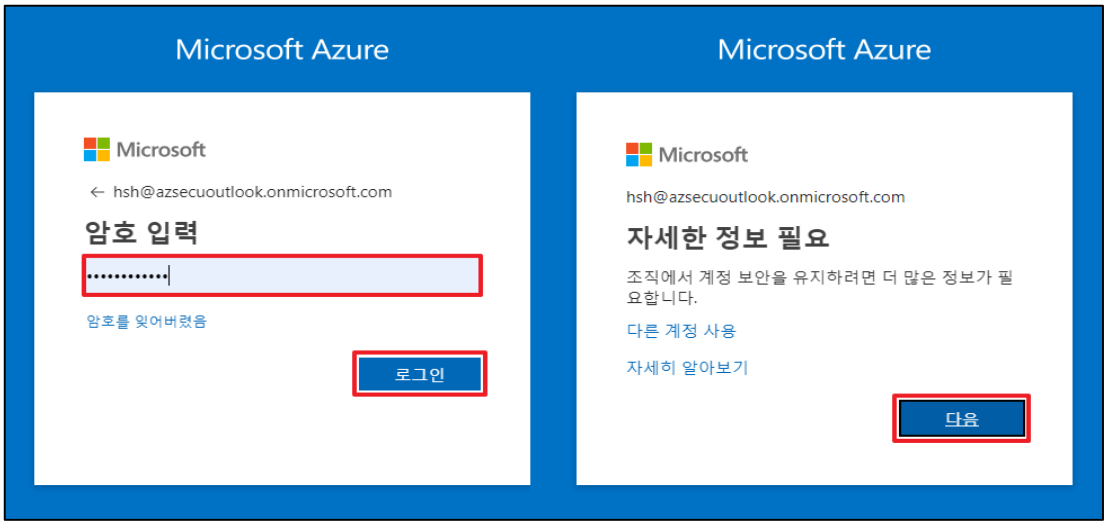


2) 모든 사용자 메뉴 내 Multi-Factor Authentication 선택

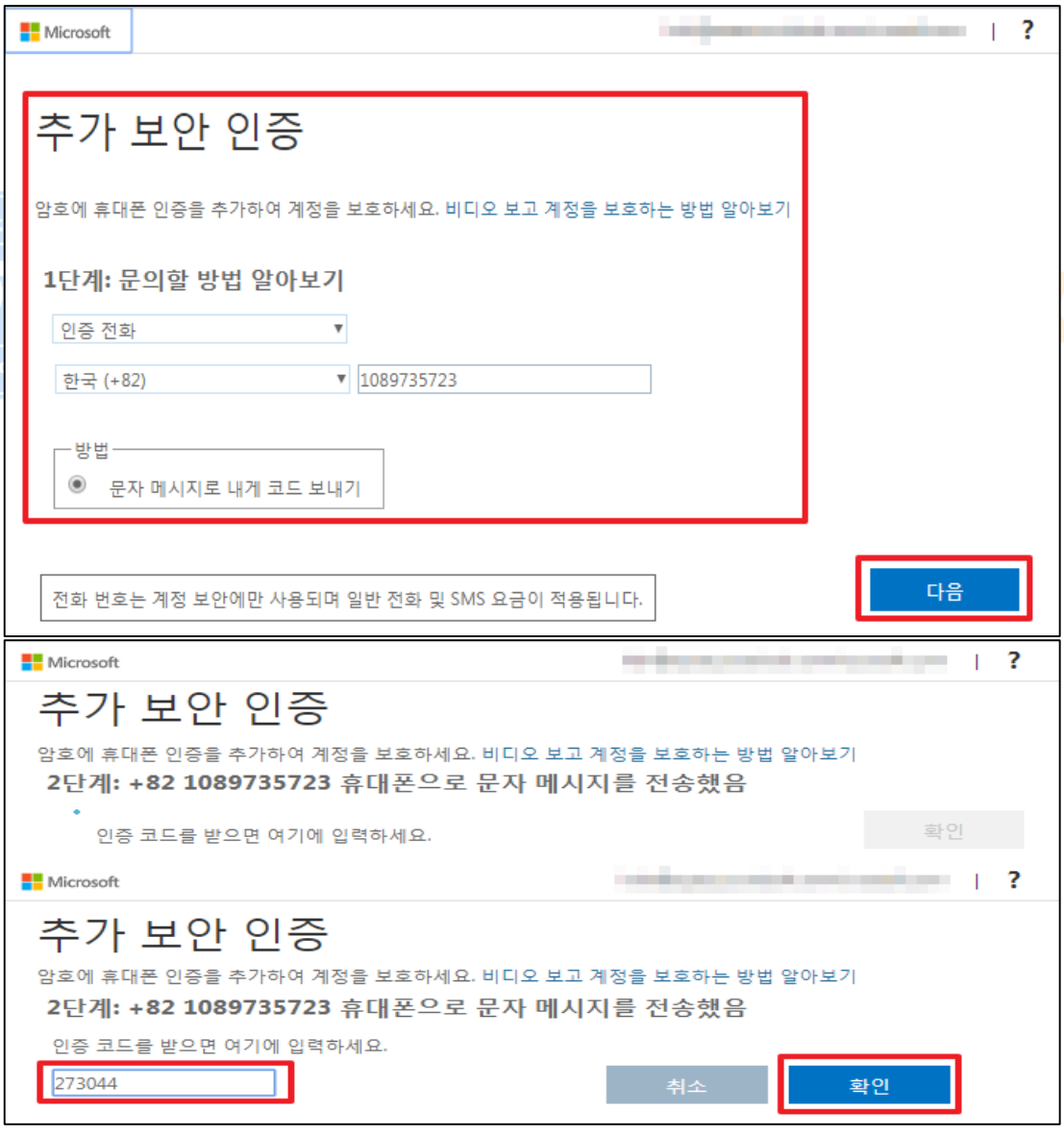
3) 다단계 인증 내 MFA를 사용할 사용자 선택 및 사용 버튼 클릭

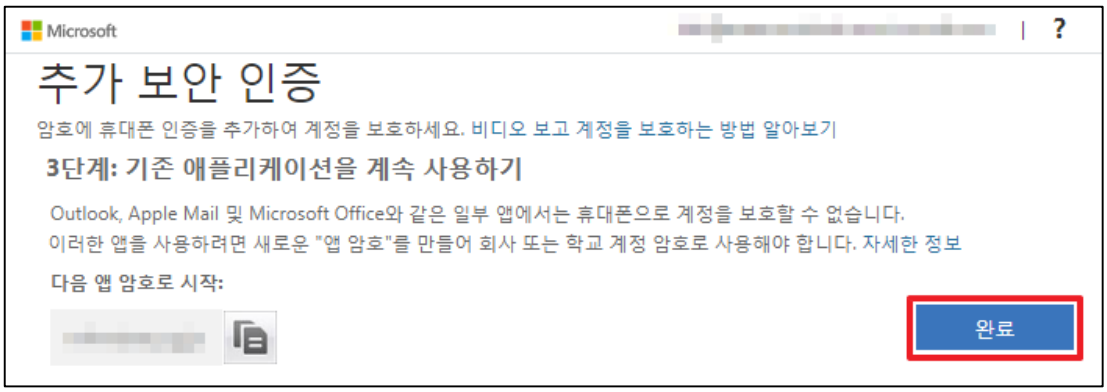


4) AD 계정으로 Azure 로그인 시도

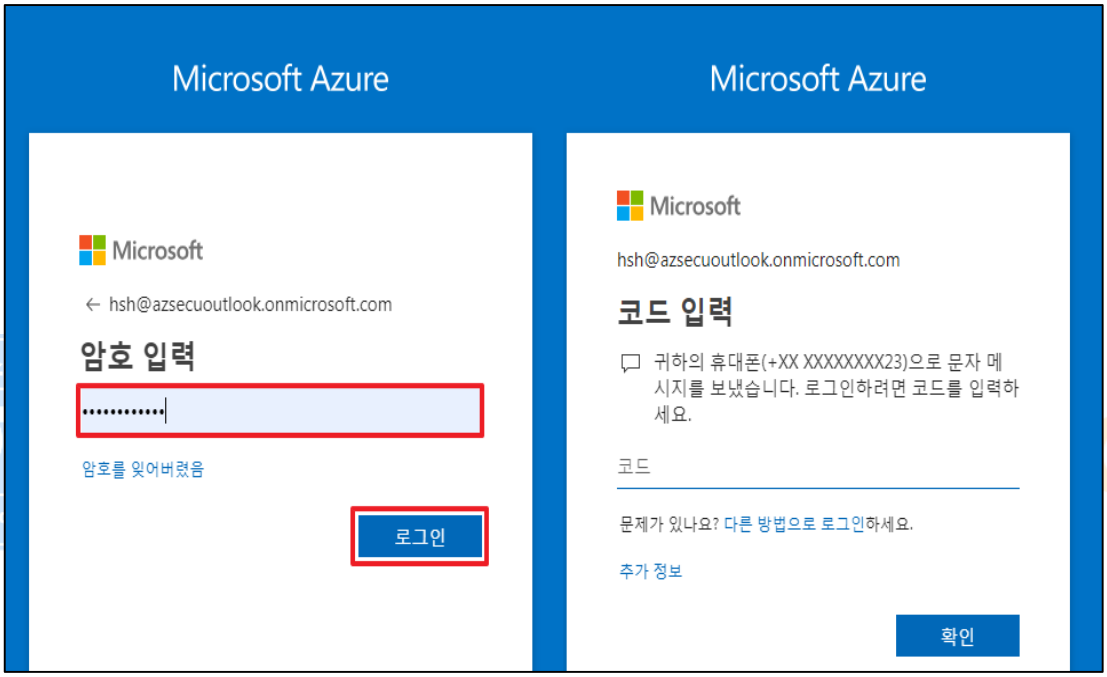


5) MFA에 사용될 보안 인증 정보(휴대폰 번호) 입력 및 본인 인증

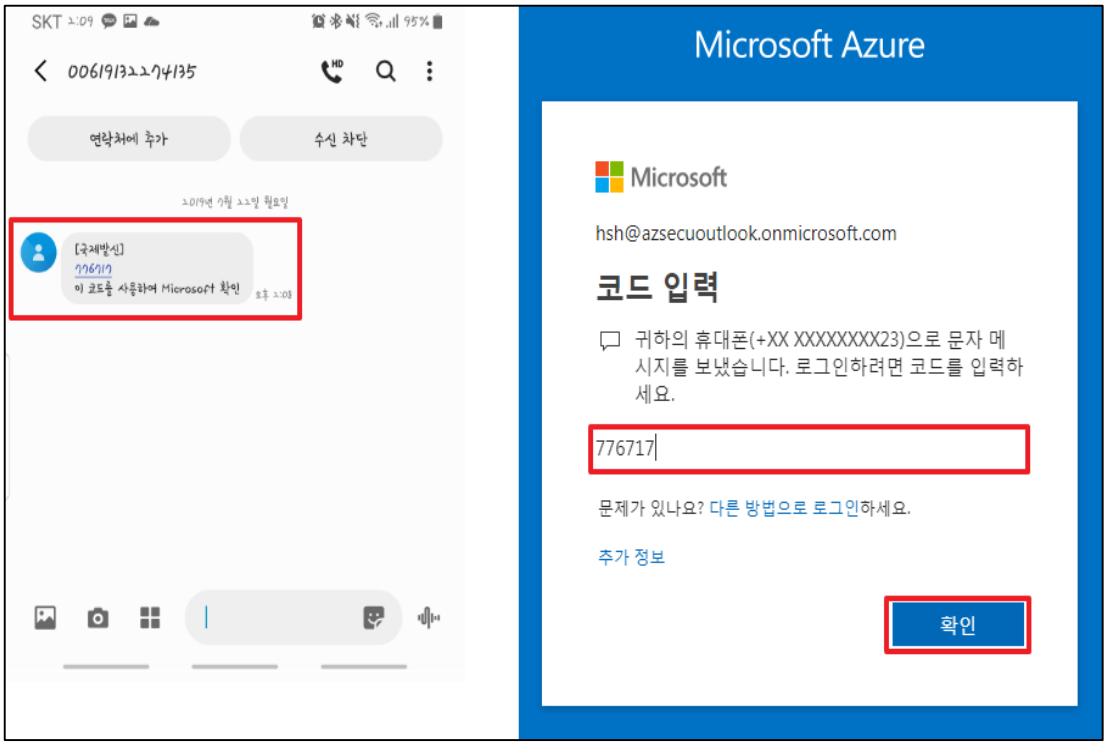




6) AD 계정으로 Azure 로그인 재진행

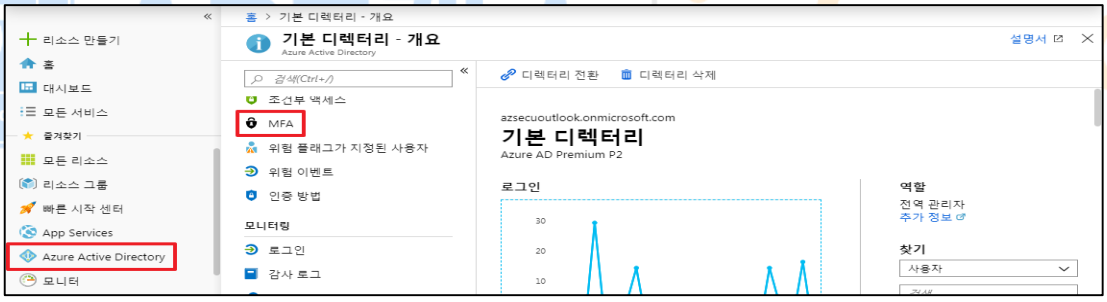


7) 휴대폰으로 발송된 인증번호 확인 및 입력 시 MFA를 통한 로그인 가능

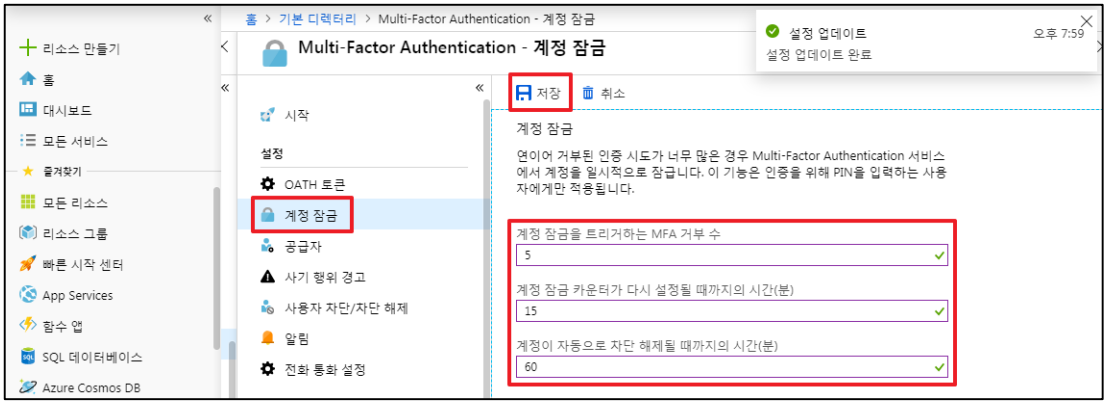


다. MFA 계정 잠금 기능 설정 방법

1) Azure Active Directory 메뉴 내 MFA 기능 선택



2) 계정 잠금 메뉴 내 값 설정 및 저장



진단 기준	양호기준 : 사용자 및 관리자 계정에 MFA를 사용하도록 설정되어 있을 경우

	취약기준 : 사용자 및 관리자 계정에 MFA를 사용하도록 설정되어 있지 않을 경우
비고	

2.7 MFA 계정 잠금 정책 관리

<table>
<tr><td>분류</td><td>계정관리</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 있습니다.
때문에 계정을 생성할 경우 패스워드 정책을 정확히 반영하여 비인가된 사용자의 악의적인 계정탈취를 방지해야 합니다.

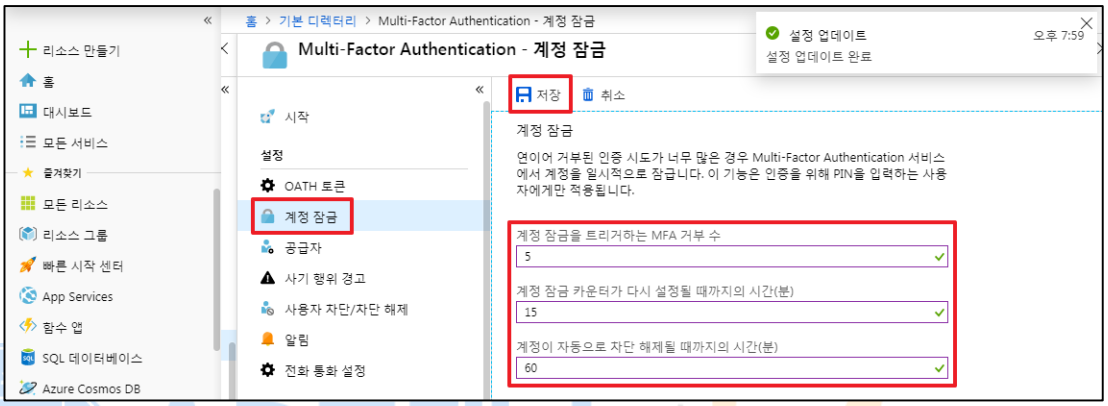
※ Multi-Factor-Authentication 계정 잠금 정책 기준
- 계정 잠금을 트리거하는MFA 거부 수 (5회)
- 계정 잠금 카운터가 다시 설정될 때까지의 시간(분) (15분)
- 계정이 자동으로 차단 해제될 때까지의 시간(분) (60분)

<패스워드 설정기준>
패스워드는 영문 대문자(26개), 영문 소문자(26개), 숫자(10개), 특수문자(32개)의 4종류
- 2종류 이상의 문자구성과 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 설정기준은 KISA "패스워드 선택 및 이용 안내서"를 참고함 (2019년 6월 개정)
https://seed.kisa.or.kr/kisa/Board/53/detailView.do

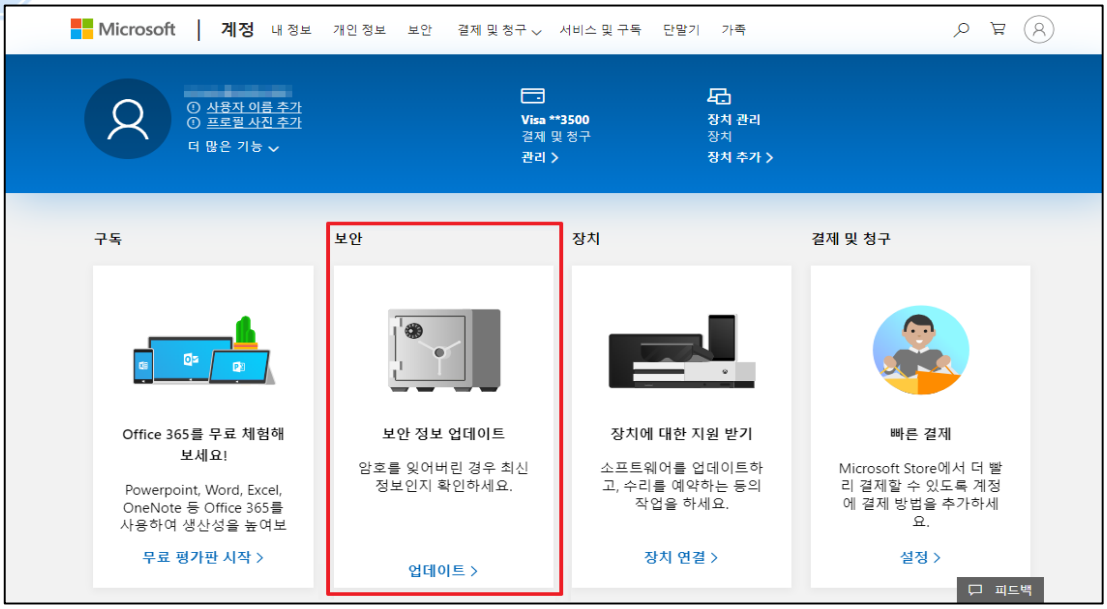
※ MS계정의 경우, 기본적으로 패스워드 복잡도 정책이 적용되어 있으며, 암호보안 설정을 통해 만기일 설정(72일)이 가능합니다.</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. MFA 계정 잠금 기능 설정 방법
1) Azure Active Directory 메뉴 내 MFA 기능 선택</td></tr>
</table>

2) 계정 잠금 메뉴 내 값 설정 및 저장

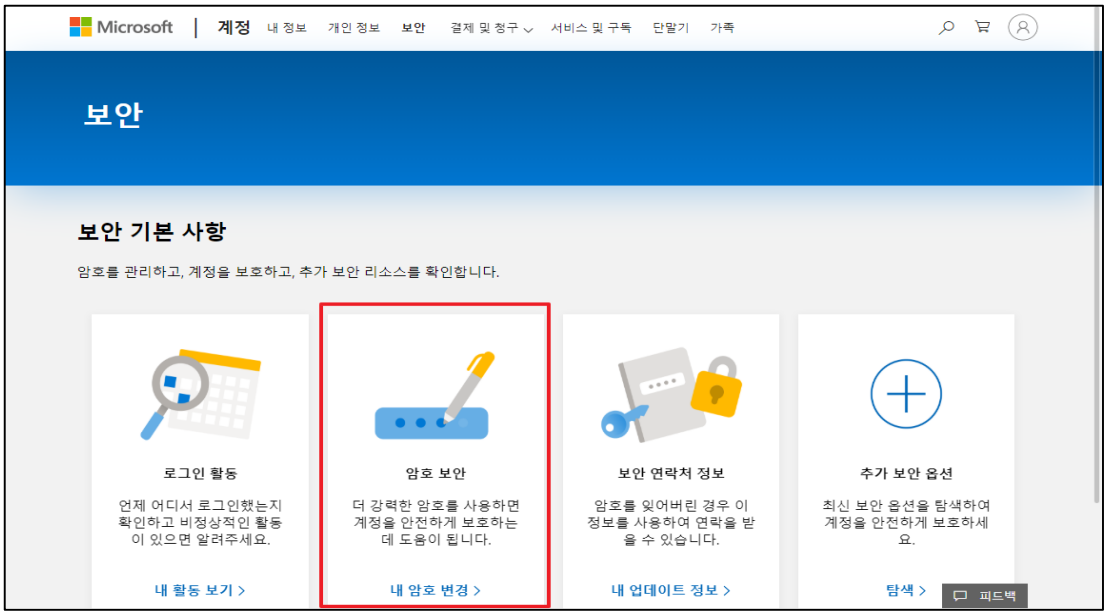


나. MS 계정 암호 사용기간 만기 시 자동변경 설정 방법

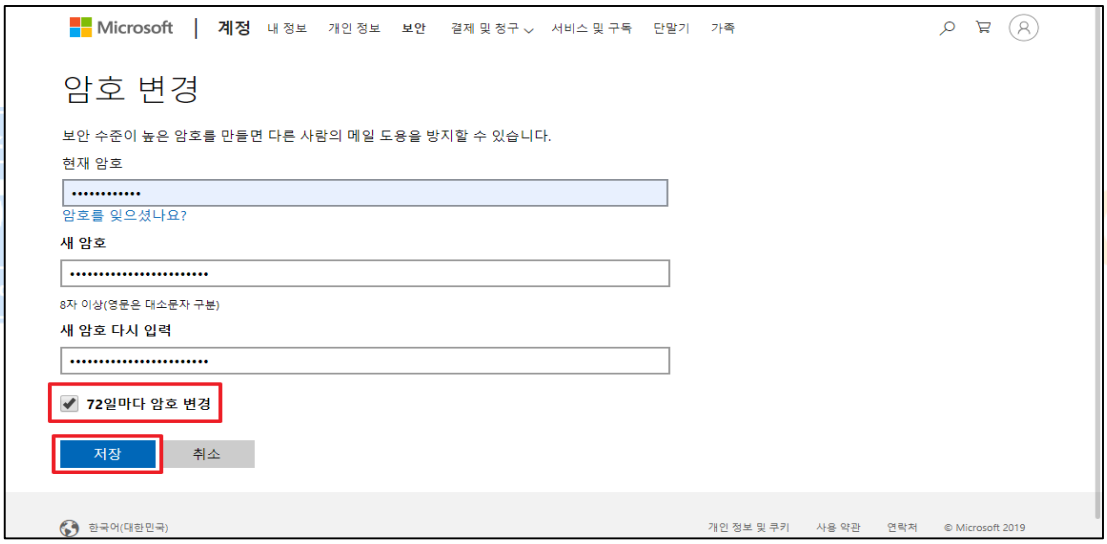
1) Microsoft 계정 메뉴 내 보안 기능 선택



2) 보안 메뉴 내 암호 보안 선택

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


3) 암호 변경 및 72일마다 암호변경 옵션 활성화 후 저장



</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: MFA구성에 계정잠금 설정이 정책에 맞게 설정되어 있을 경우

취약기준
: MFA구성에 계정잠금 설정이 정책에 맞게 설정되어 있지 않을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

2.8 Azure 패스워드 정책 관리

분류	계정관리	중요도	중
항목명	Azure 패스워드 정책 관리		

항목 설명

Azure AD(Activie Directory)에서 제공하는 인증방법을 통해 인증정책을 설정하거나, 암호보호 정책을 설정할 수 있습니다. 인증방법 정책은 전체 또는 일부 사용자에게 암호없는 인증을 사용하도록 설정하는 기능이며, 암호보호 정책은 조직의 암호정책을 강화할 수 있습니다.

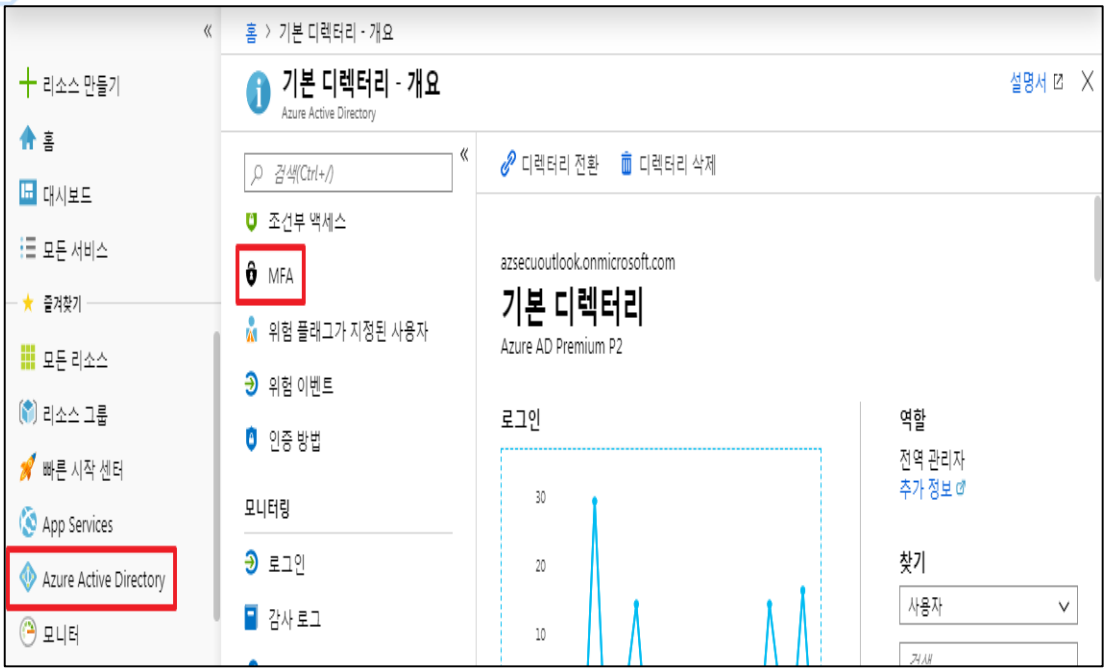
※ AD 인증방식 암호보호 정책

설정	내용	기준값
잠금 임계값	로그인 실패 시 허용 횟수	5회
잠금 시간(초)	계정 최초 잠금 시 잠금시간이며, 실패횟수가 증가할수록 잠금시간은 증가함.	3600초
사용자 지정 금지된 암호	추측하기 쉬운 암호의 사용을 금지하기 위해 암호 시스템에 관리자가 등록한 금지암호를 등록	사용자 정의
Windows 서버 AD에 대한 암호보호	온-프레미스와 통합되어 있을 경우, Azure AD의 안전한 암호배포를 위해 에이전트를 설치	예
모드	사용자 지정 금지된 암호를 사용할 경우 사용금지(적용됨) 또는 로그만 기록(감사)	적용됨

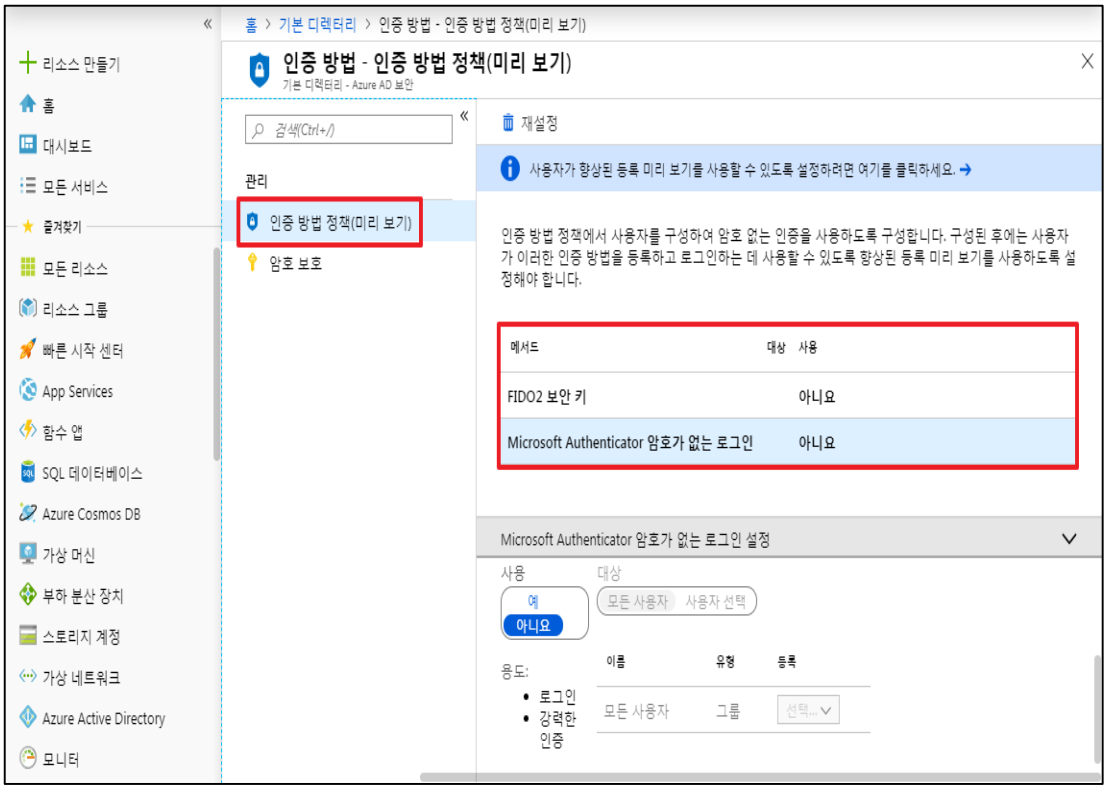
설정 방법

가. 비암호 로그인 방지 설정 방법

1) Azure Active Directory 메뉴 내 MFA 기능 선택

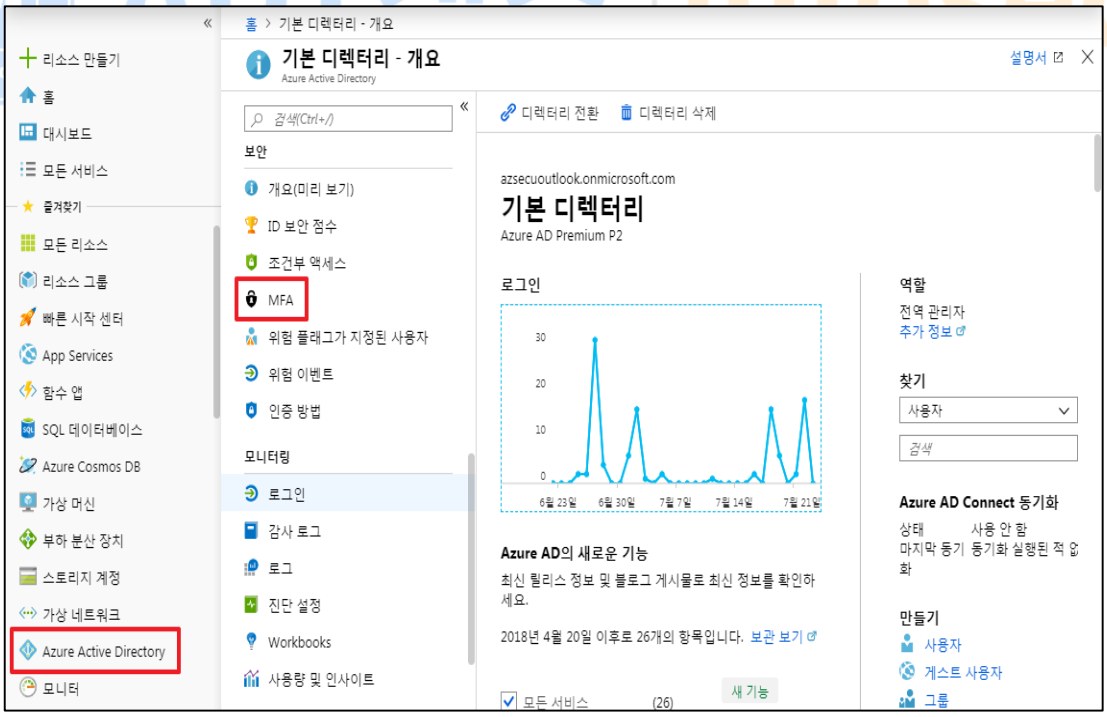


2) 인증 장법 정책(미리 보기) 메뉴 내 FIDO2 보안 키, MS –Authenticator 비암호 로그인 설정

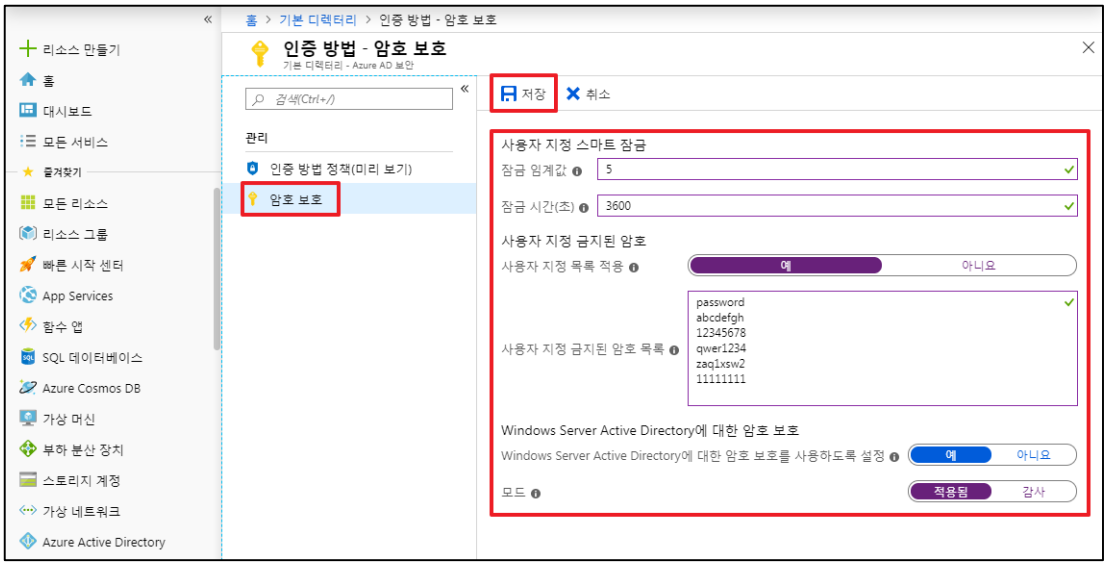


나. 로그인 정책 설정 방법

1) Azure Active Directory 메뉴 내 MFA 기능 선택

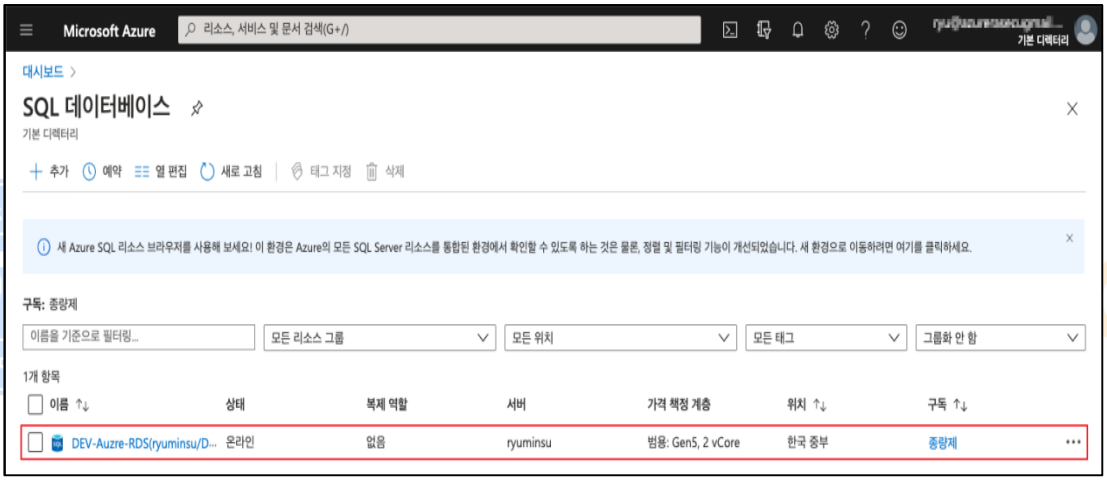
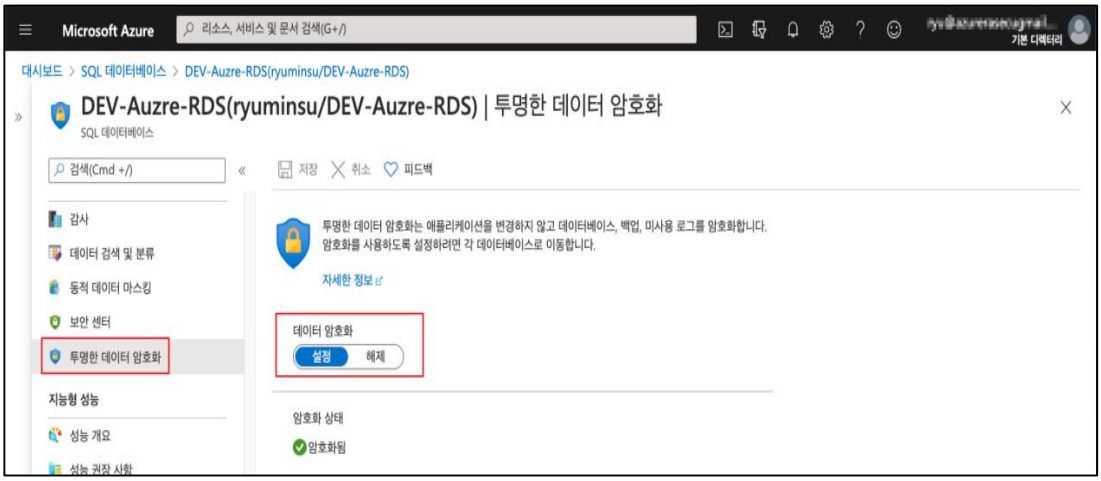


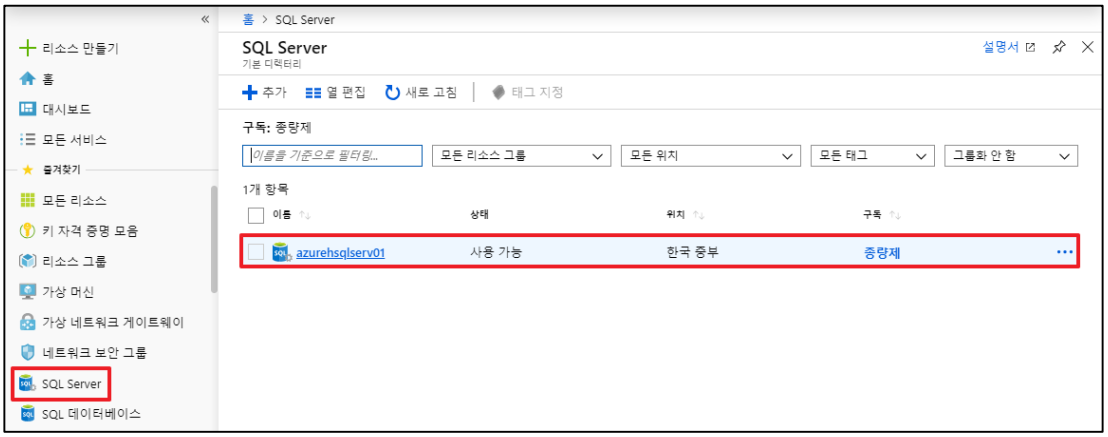
2) 암호 보호 메뉴 내 사용자 지정 스마트 잠금 설정

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

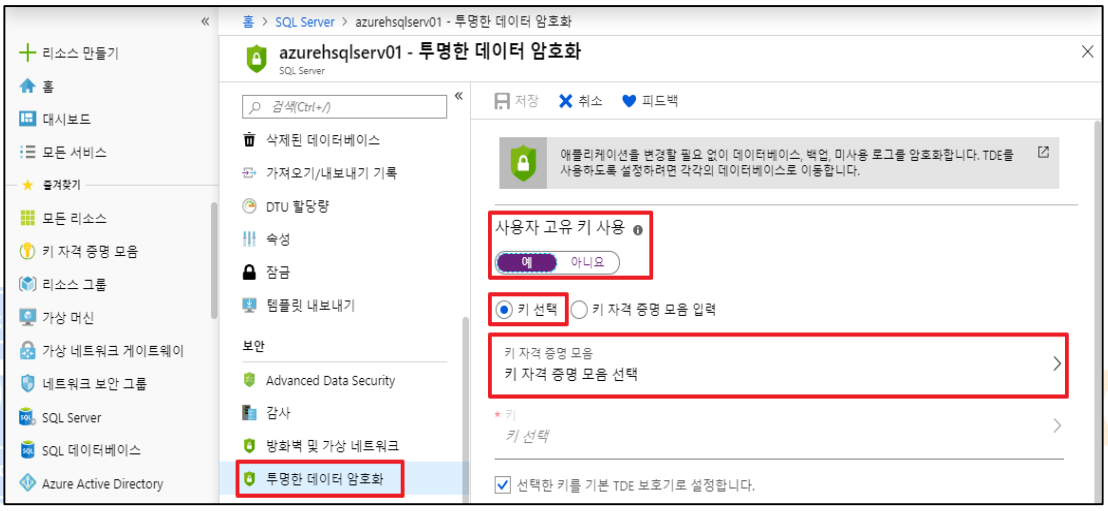
3. 데이터관리

3.1 투명한 데이터 암호화 (TDE)

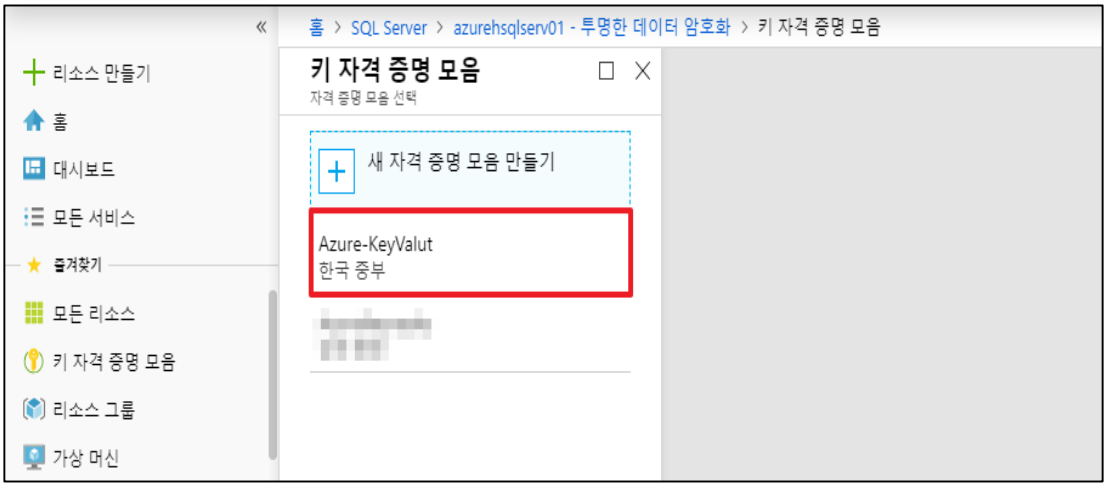
분류	데이터 관리	중요도	중
항목명	투명한 데이터 암호화 (TDE)		
항목 설명	투명한 데이터 암호화 (TDE)는 SQL서버, 데이터베이스 등에서 미사용 데이터를 암호화 하여 오프라인 활동으로부터 데이터를 보호하는 기법입니다. TDE는 애플리케이션에 대한 변경없이 미사용 데이터베이스, 연결된 백업 및 트랜잭션 로그파일의 실시간 암호화 및 암호해독을 수행합니다. 기본적으로 활성화 된 SQL 데이터베이스에는 TDE 설정이 활성화 되어 있으며, SQL서버의 경우 Key Vault를 사용한 사용자 고유키를 설정할 수 있으며 고유키의 만료일자 설정을 통해 제한적으로 사용으로 보안성을 보다 더 높일 수 있습니다.		
설정 방법	**가. SQL 데이터베이스 투명한 데이터 암호화 (TDE) 설정 방법** 1) SQL 데이터베이스 메뉴 내 데이터 암호화 (TDE)를 설정할 데이터베이스 선택  2) 투명한 데이터 암호화 메뉴 내 데이터 암호화 설정 및 저장 후 암호화 상태 확인  **나. SQL 서버 투명한 데이터 암호화(TDE) 설정 방법** 1) SQL 서버 메뉴 내 데이터 암호화(TDE)를 설정할 SQL 서버 선택		



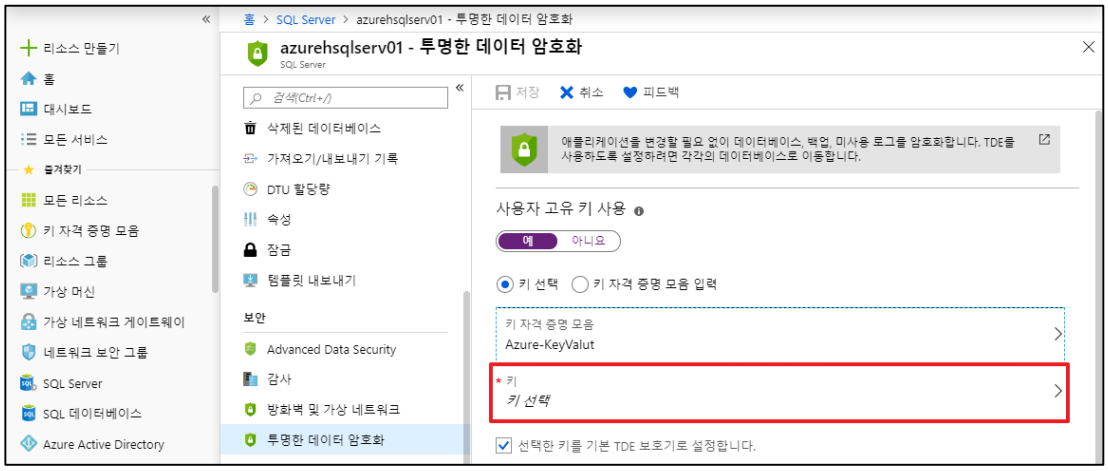
2) 투명한 데이터 암호화 메뉴 내 사용자 고유 키 사용 옵션 활성화 및 주요 자격 증명 모음 설정



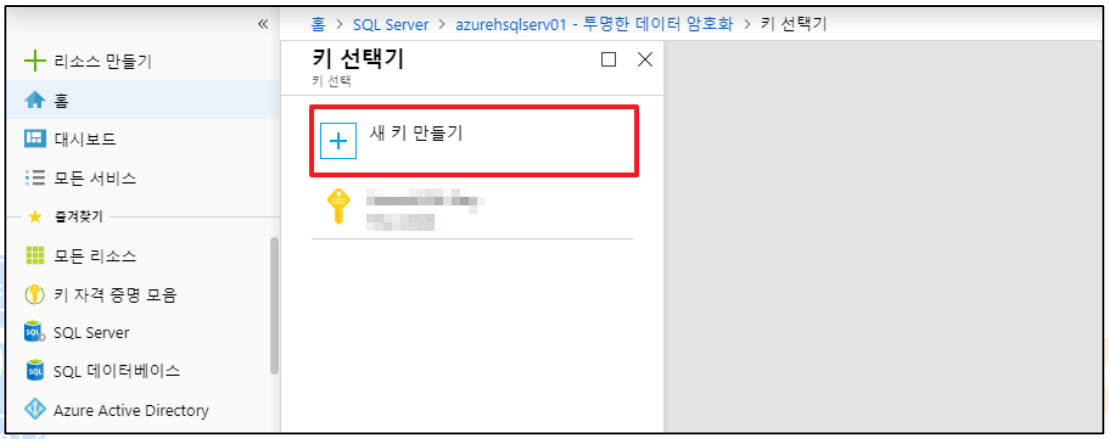
3) 암호화에 사용할 사용할 키 자격 증명 모음 선택



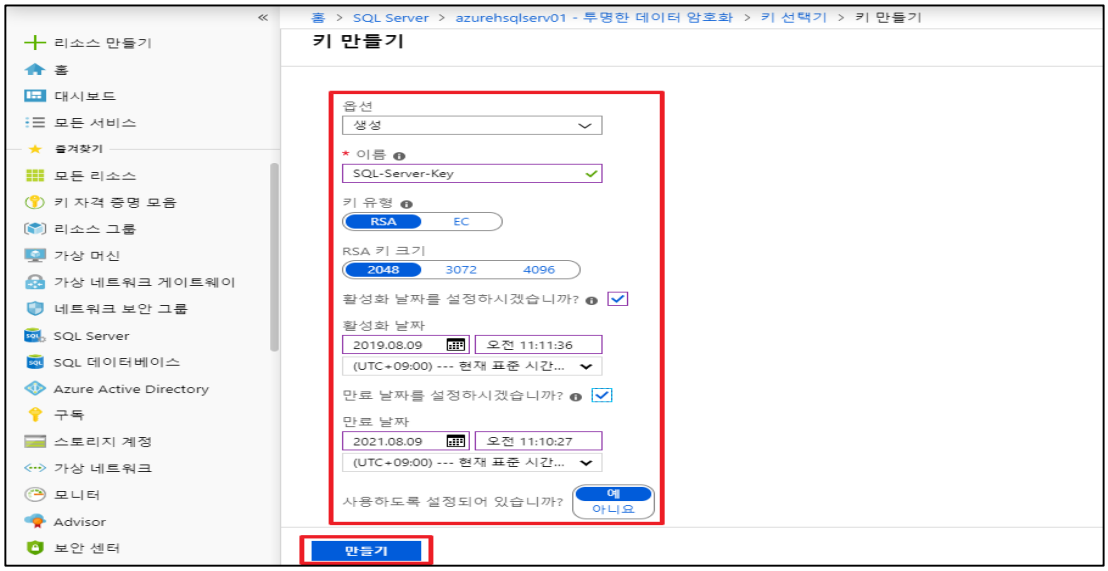
4) 암호화 메뉴 내 사용할 암호화 키 선택



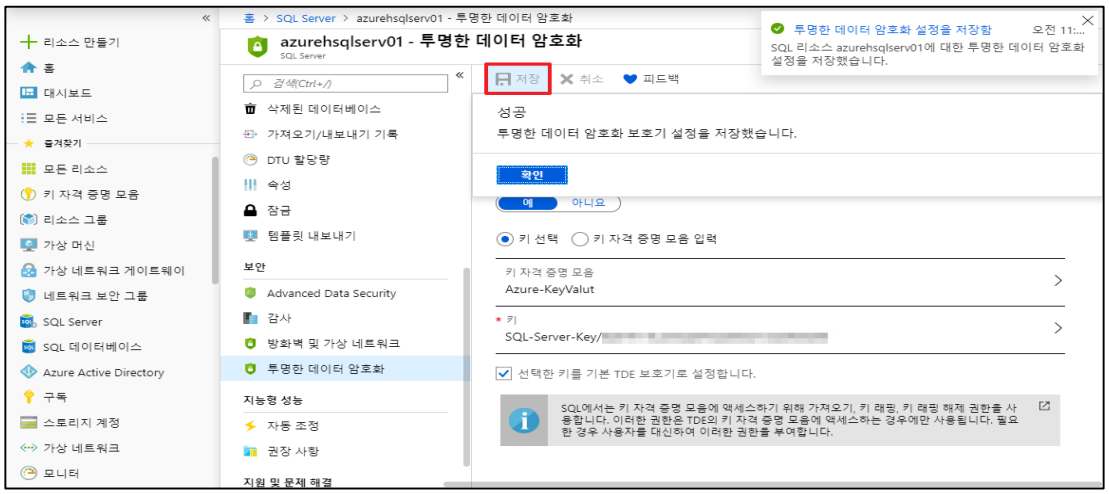
5) 기존에 생성된 키가 없거나 별도로 관리할 경우 새 키 만들기 선택



6) 키 생성 관련 옵션(키 유형, 키 크기, 키 활성화 날짜, 키 만료 날짜) 설정 및 만들기



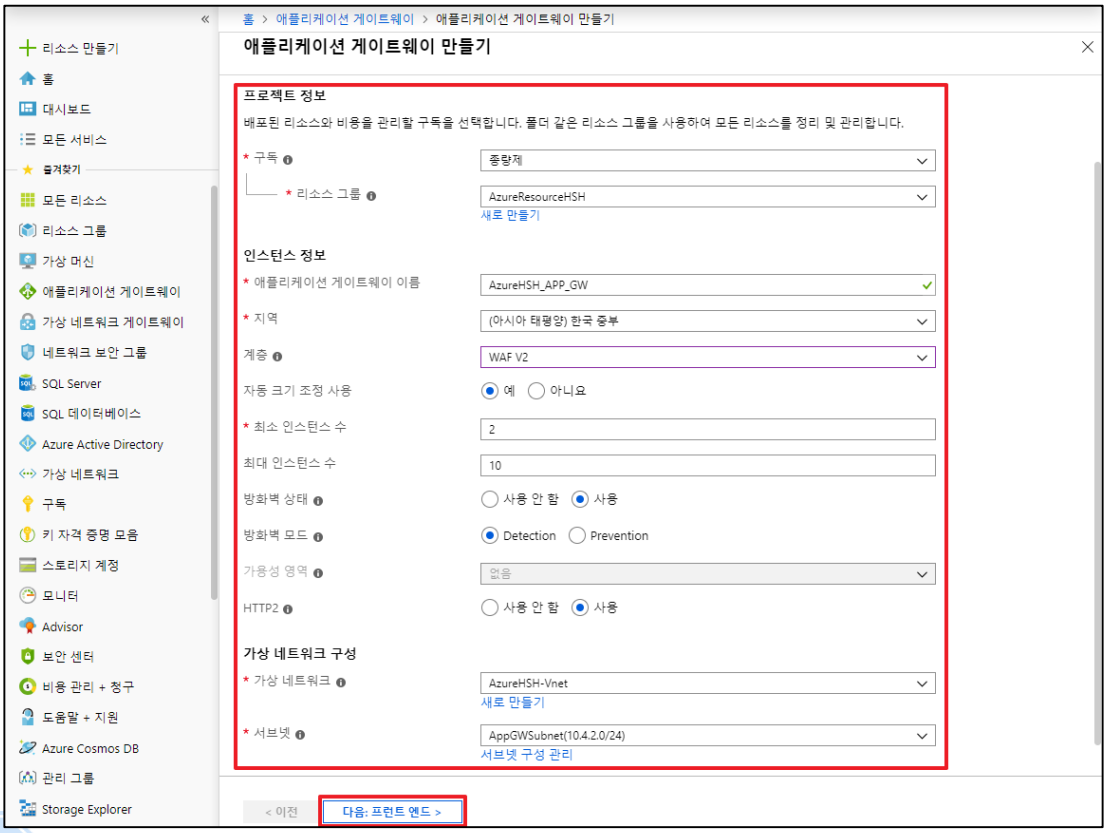
7) 암호화 설정 및 저장

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: SQL서버 및 데이터베이스에 투명한 데이터 암호화 기능을 사용하도록 설정되어 있을 경우

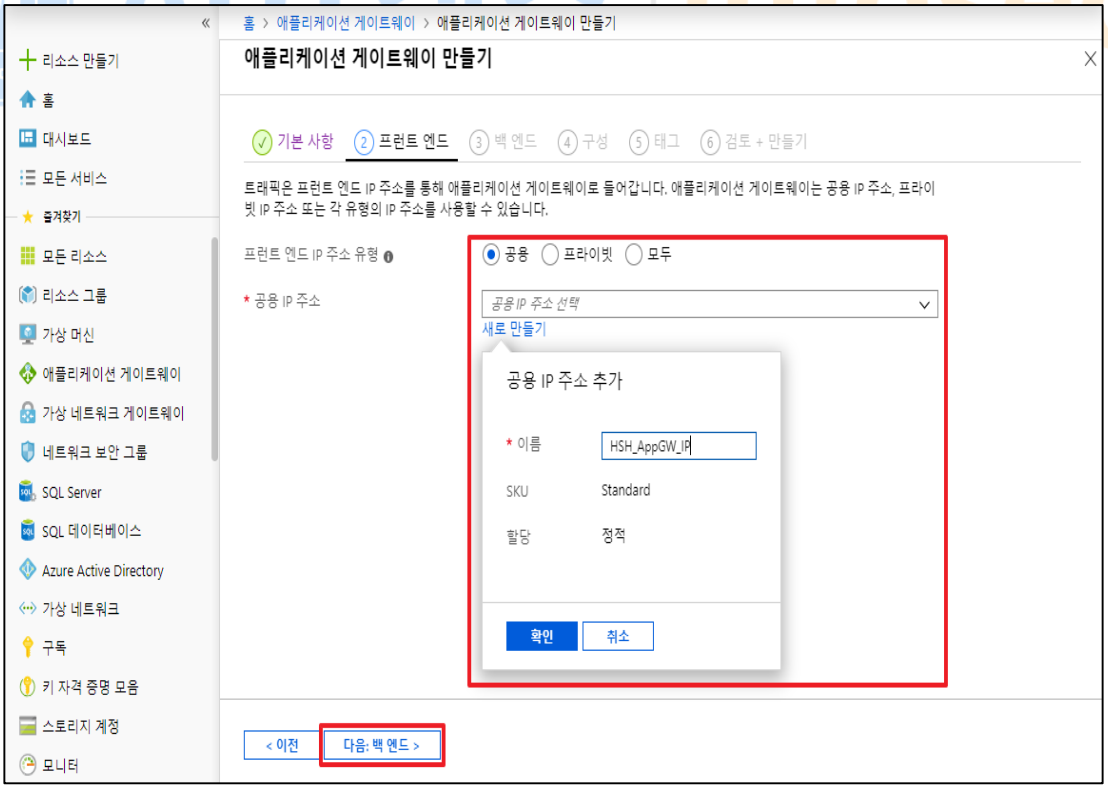
취약기준
: SQL서버 및 데이터베이스에 투명한 데이터 암호화 기능을 사용하도록 설정되어 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3.2 애플리케이션 게이트웨이 암호화

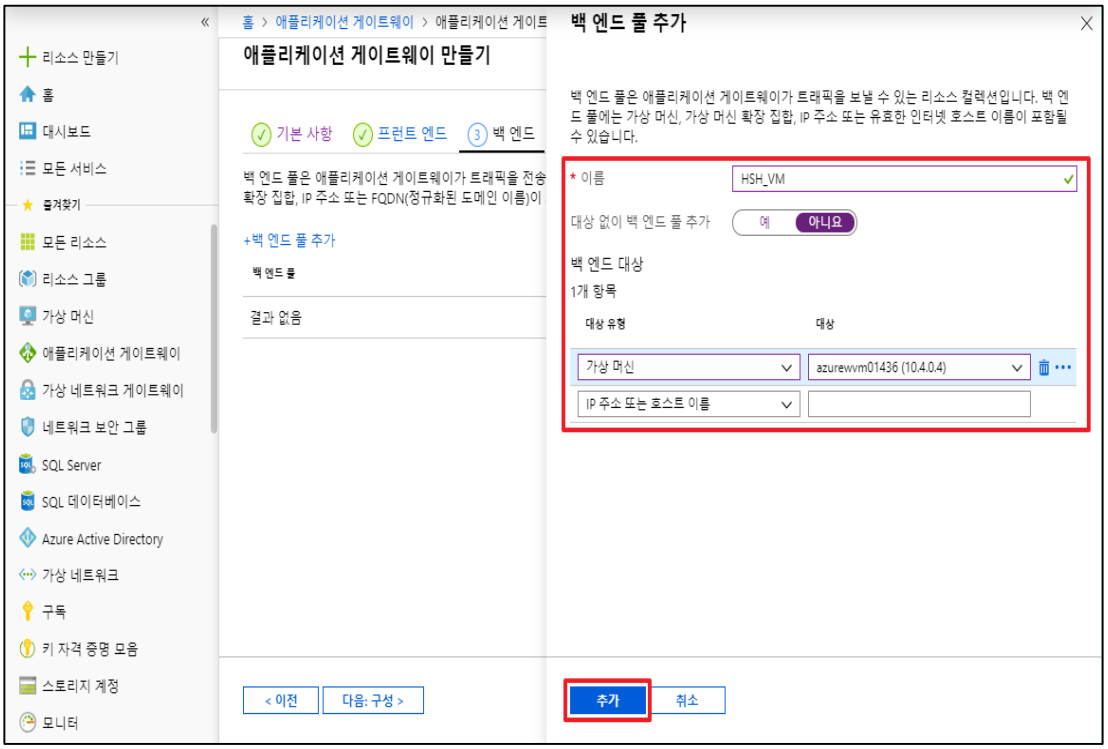
분류	데이터 관리	중요도	상
항목명	애플리케이션 게이트웨이 암호화		
항목 설명	애플리케이션 게이트웨이는 웹 애플리케이션에 대한 트래픽을 관리할 수 있도록 하는 웹 트래픽 부하분산 장치로 URI 경로 / 호스트 헤더 / HTTP 요청의 추가특성을 기반으로 라우팅 결정을 내릴 수 있습니다. 또한 일반적인 악용 및 취약점으로부터 웹 애플리케이션에 대해 중앙 집중화 된 보호를 제공하는 WAF(웹 애플리케이션 방화벽) 기능도 함께 제공합니다. 특히, 중요/민감정보를 송/수신해야 하는 웹 애플리케이션에 대해 엔드포인트에 최소 TLS 1.2 이상 사용할 경우에만 요청을 허용하도록 설정할 수 있습니다. 이를 통해 네트워크 상에 평문으로 노출되는 이슈를 예방할 수 있으며, 암호화 및 암호해독에 대한 오버헤드로부터 웹 서버의 부담을 줄여줄 수 있습니다		
설정 방법	**가. 애플리케이션 게이트웨이 설정 방법** 1) 애플리케이션 게이트웨이 메뉴 내 추가 및 게이트웨이 만들기 버튼 선택  2) 애플리케이션 게이트웨이 관련 값 설정		



3) 프런트 엔드 값 설정

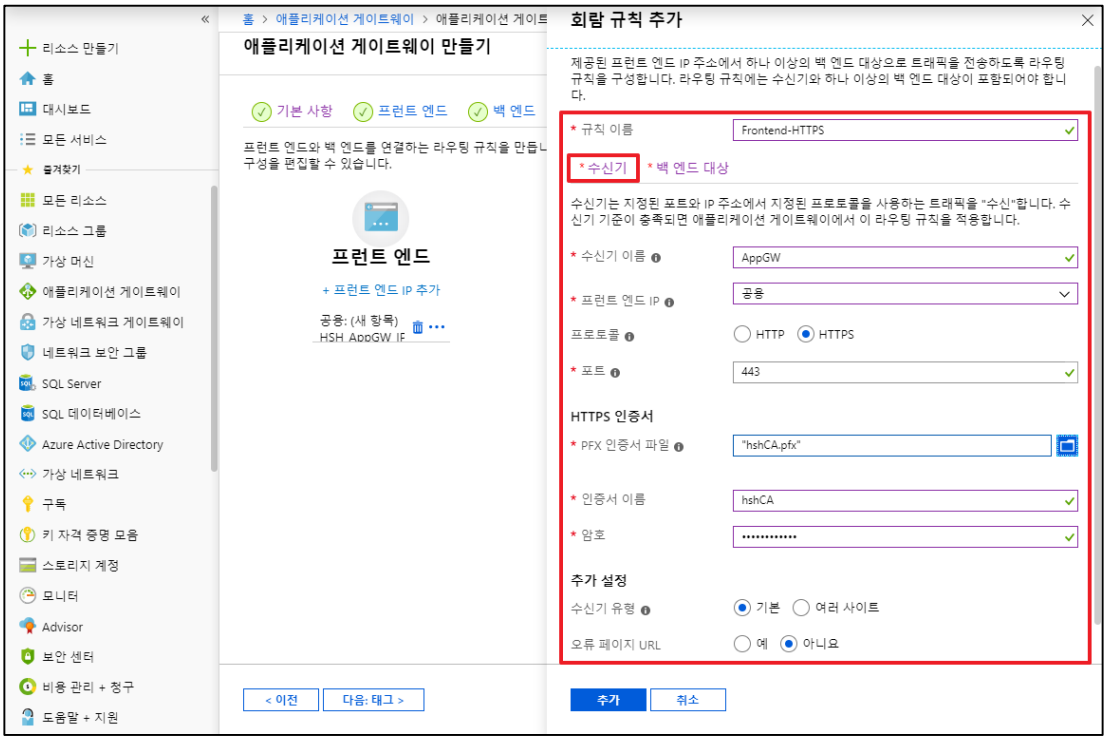


4) 백 엔드 풀 값 설정

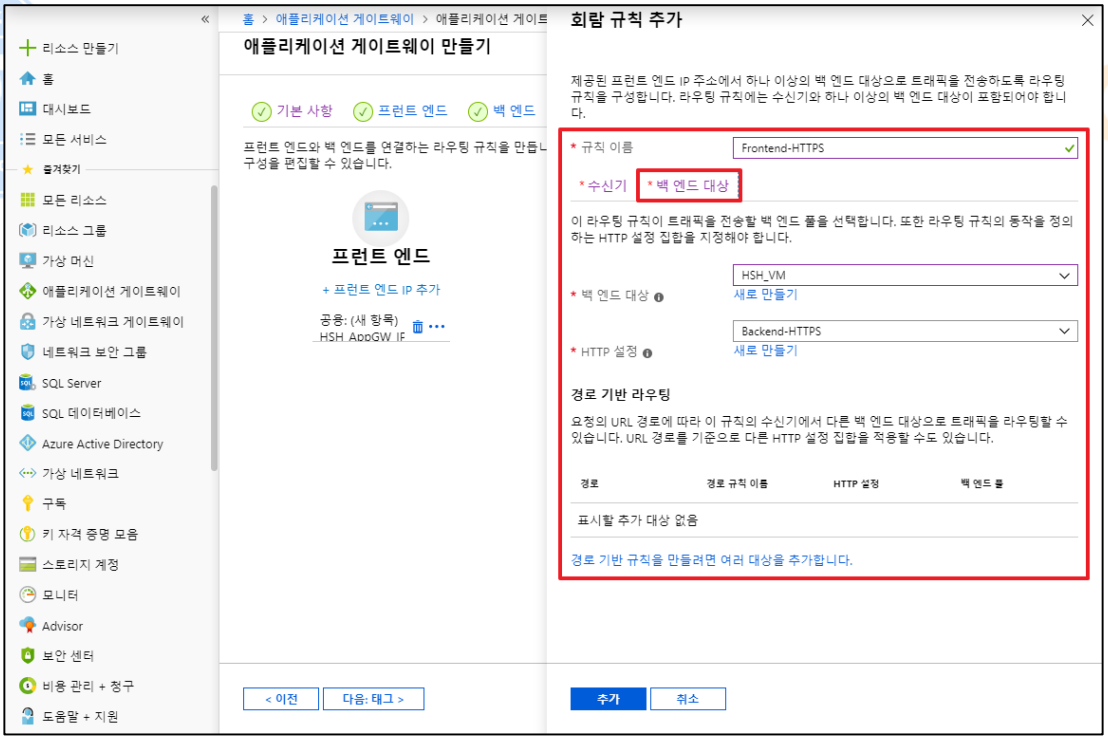


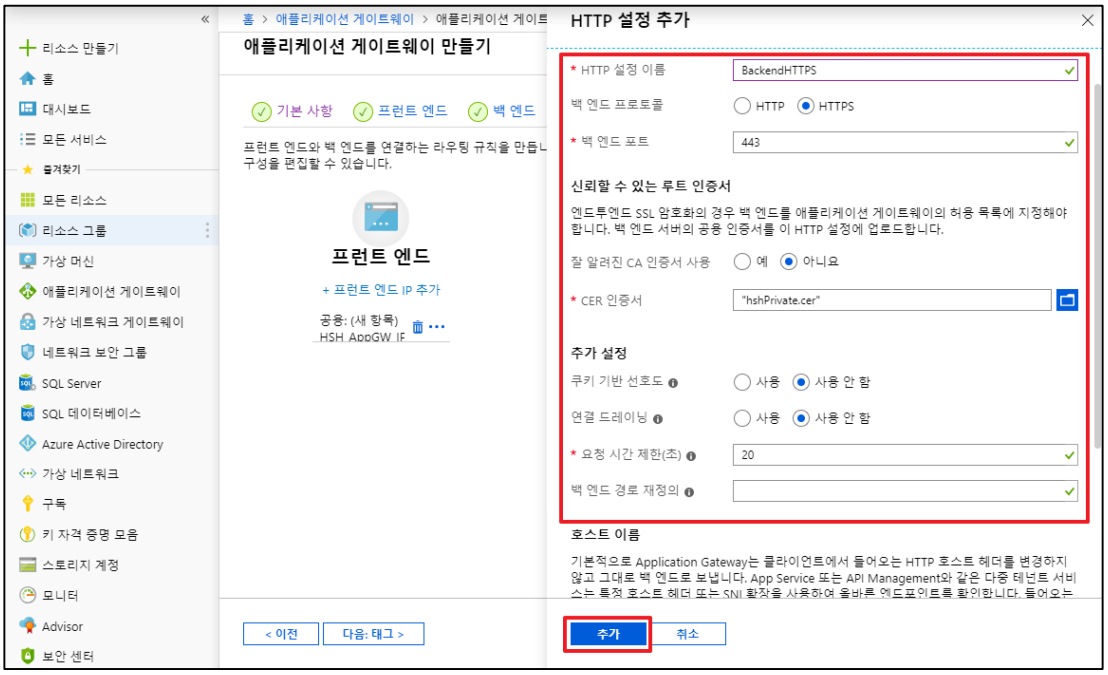
5) 회람규칙 추가 버튼 선택

6) 수신기 값 및 통신(HTTPS) 규칙 설정



7) 백 엔드 대상 및 통신(HTTPS) 규칙 설정





8) 생성된 규칙/정보 검토 및 만들기

진단 기준

양호기준

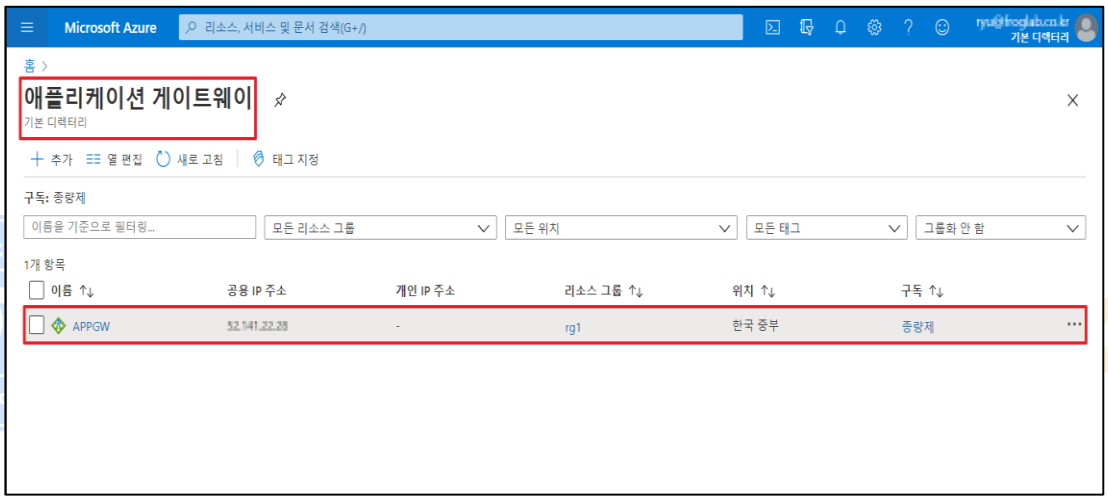
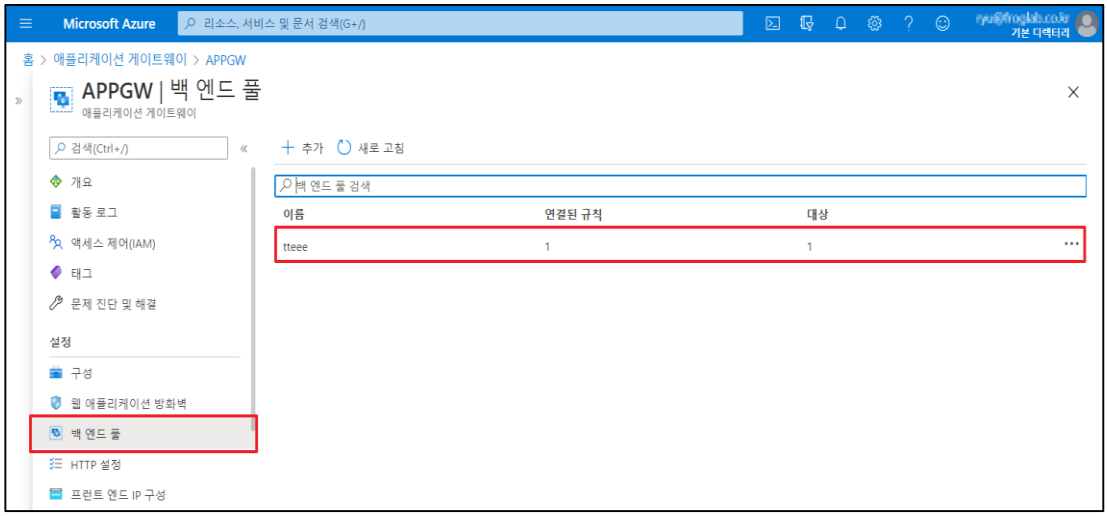
: 회람규칙의 허용 프로토콜이 HTTPS로 설정되어 있을 경우

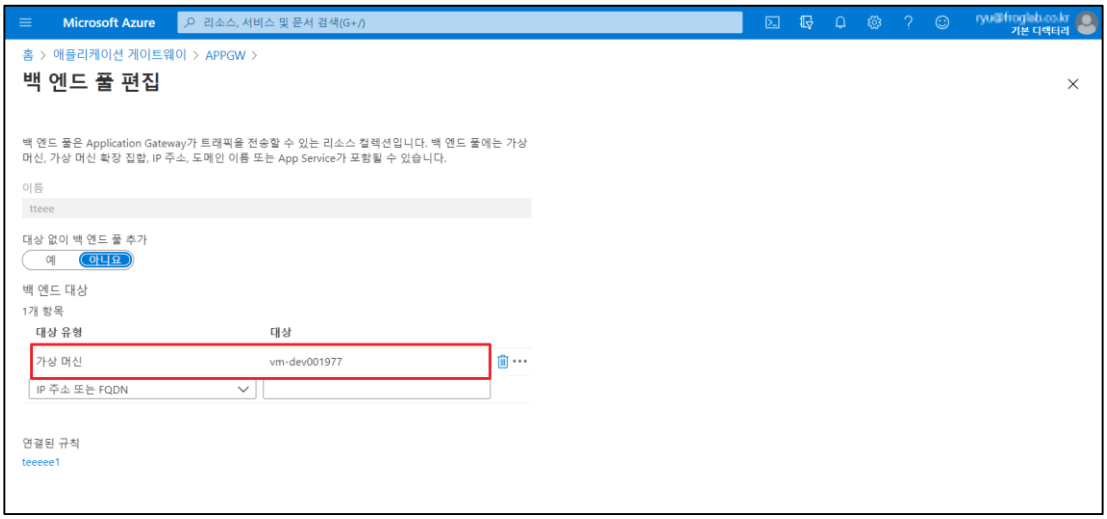
취약기준

: 회람규칙의 허용 프로토콜이 HTTPS로 설정되어 있지 않을 경우

비고

3.3 애플리케이션 게이트웨이 풀 관리

분류	데이터 관리	중요도	중
항목명	애플리케이션 게이트웨이 풀 관리		
항목 설명	애플리케이션 게이트웨이는 웹 애플리케이션에 대한 트래픽을 관리할 수 있도록 하는 웹 트래픽 부하분산 장치로 URI 경로 / 호스트 헤더 / HTTP 요청의 추가특성을 기반으로 라우팅 결정을 내릴 수 있습니다. 또한 일반적인 악용 및 취약점으로부터 웹 애플리케이션에 대해 중앙 집중화 된 보호를 제공하는 WAF(웹 애플리케이션 방화벽) 기능도 함께 제공합니다. 애플리케이션 게이트웨이에 연결된 백 엔드 풀 대상 중 불필요한 리소스가 존재하는 경우 AZURE 리소스에 비정상적인 접근 또는 2차 공격에 활용될 수 있습니다.		
설정 방법	**가. 애플리케이션 게이트웨이 백엔드 풀 대상 확인방법** 1) 대상 애플리케이션 게이트웨이 접근  2) 백 엔드 풀에 지정된 규칙 상세보기  3) 연결된 대상 확인 및 필요여부 검증		

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: 백 엔드 풀 대상에 불필요한 대상이 연결되어 있지 않을 경우

취약기준
: 백 엔드 풀 대상에 불필요한 대상이 연결되어 있을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3.4 Key Vault 암호화 설정

분류	데이터 관리	중요도	상
항목명	Key Vault 암호화 설정		

항목 설명

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 SQL Server TDE(투명한 데이터 암호화) 설정 및 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.

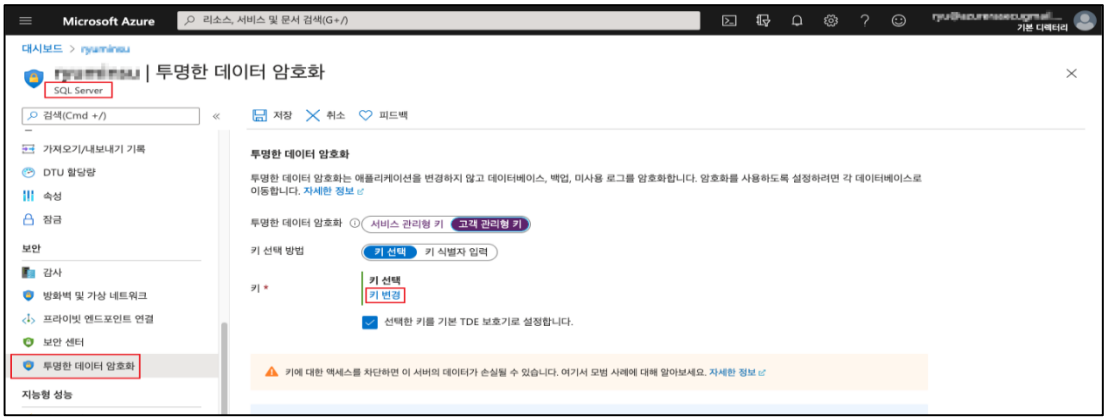
(*) 암호화 키 관리 옵션

키 관리 매개 변수	Microsoft 관리형 키	고객 관리형 키	고객이 제공한 키
암호화/암호 해독 작업	Azure	Azure	Azure
지원되는 Storage 서비스	모두	Blob, Files	Blob
키 스토리지	Microsoft 키 저장소	Key valut 또는 HSM	고객의 고유 키 저장소
키 회전 책임	Microsoft	Customer	Customer
키 컨트롤	Microsoft	Customer	Customer

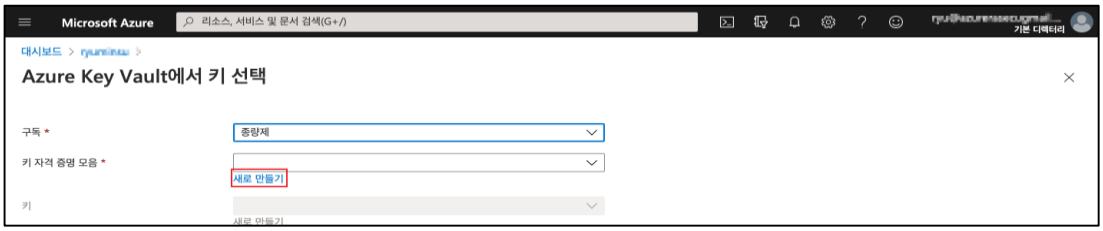
설정 방법

가. SQL Server 투명한 데이터 암호화 및 만료일자 설정

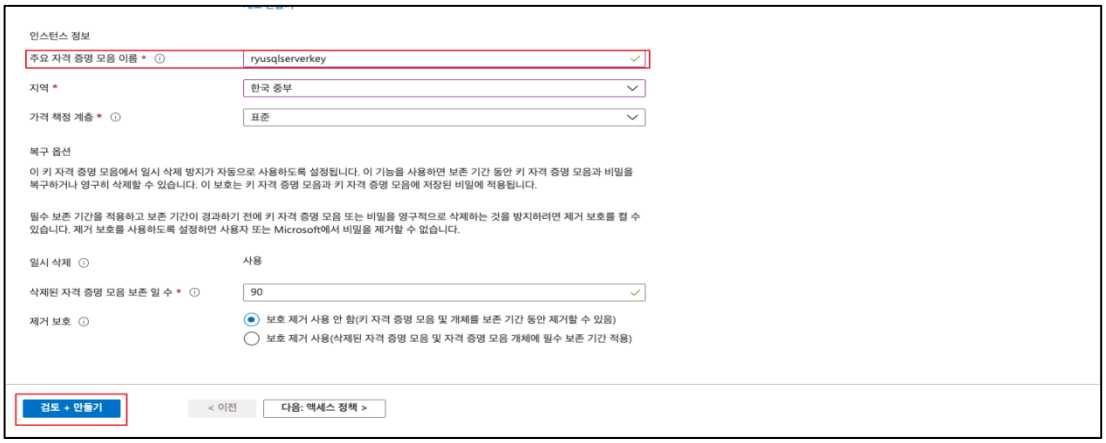
1) 투명한 데이터 암호화 키 변경 클릭



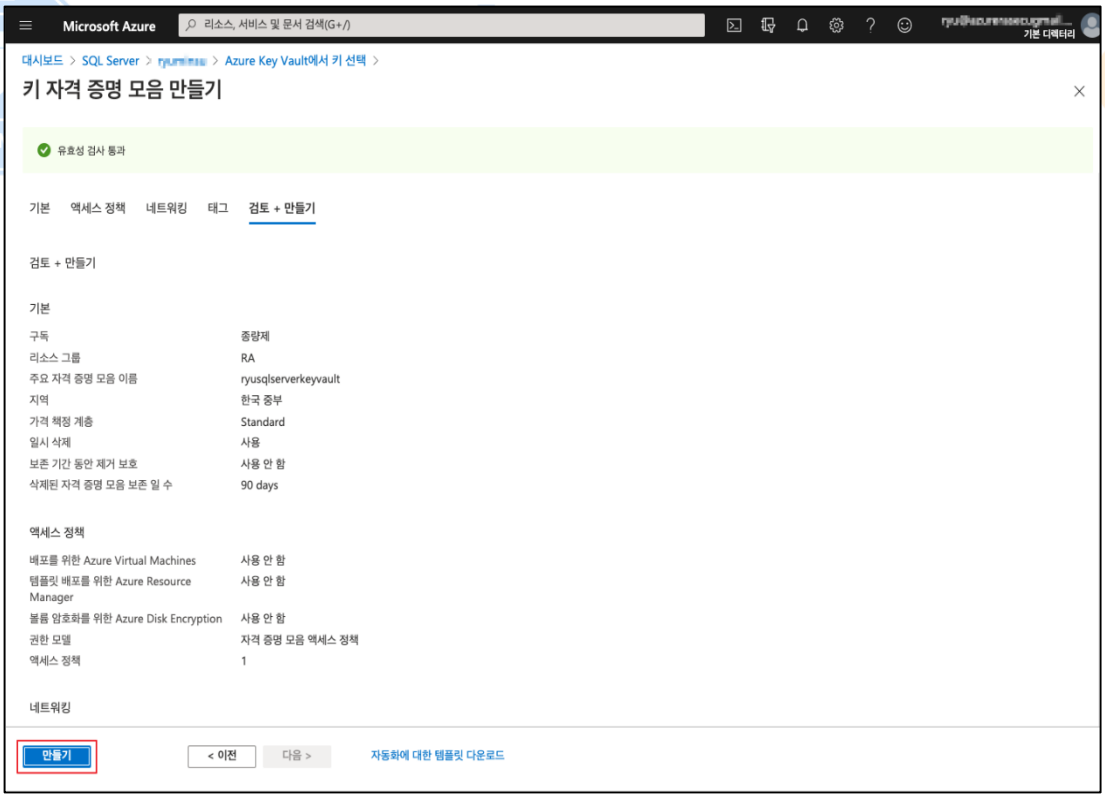
2) Azure key Vault 키 자격모음 만들기 선택



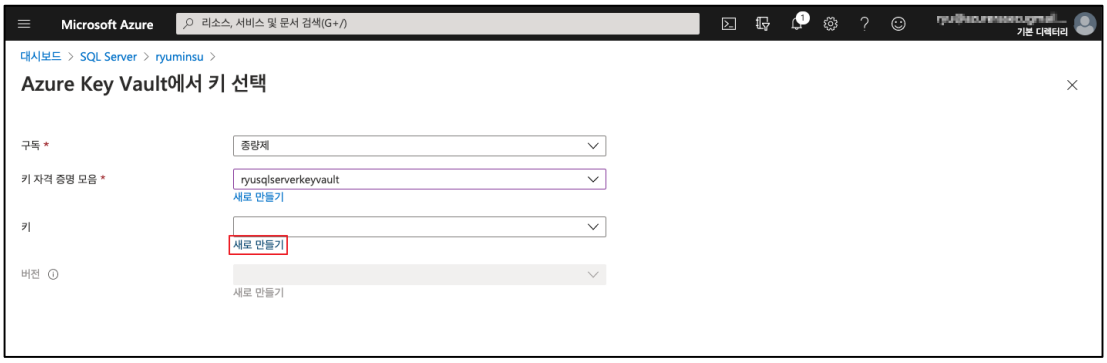
3) Azure key Vault 키 자격모음 만들기



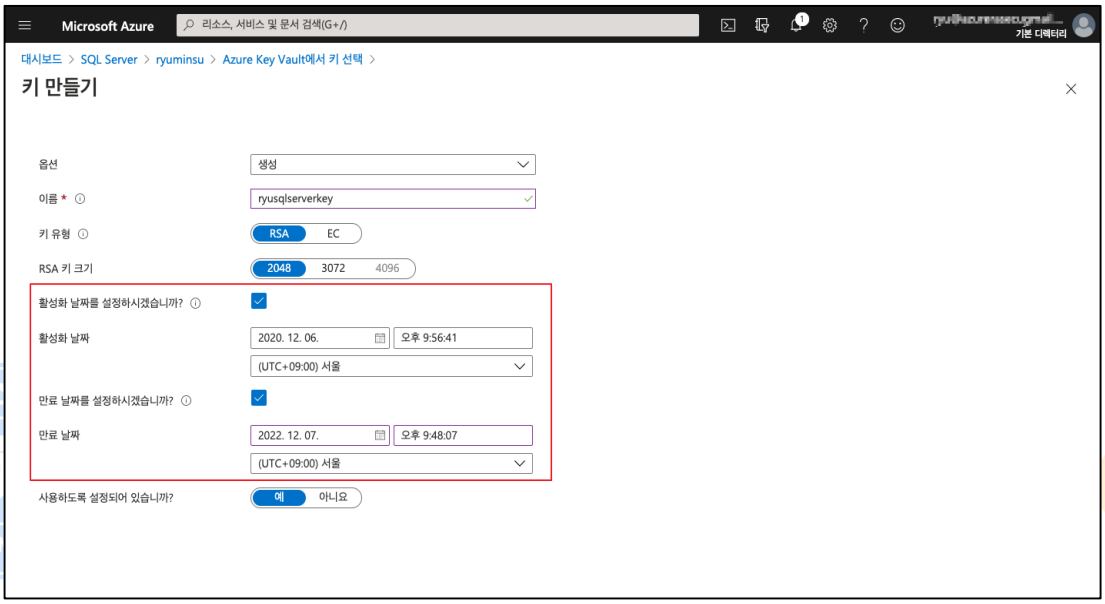
4) Azure key Vault 키 자격모음 만들기 완료



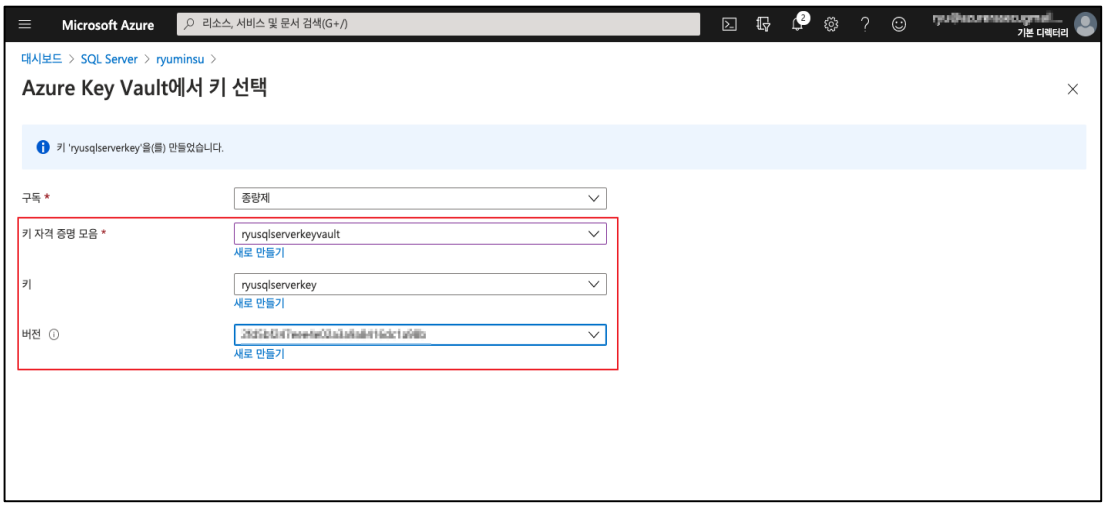
5) Azure key Vault 키 새로 만들기 시도



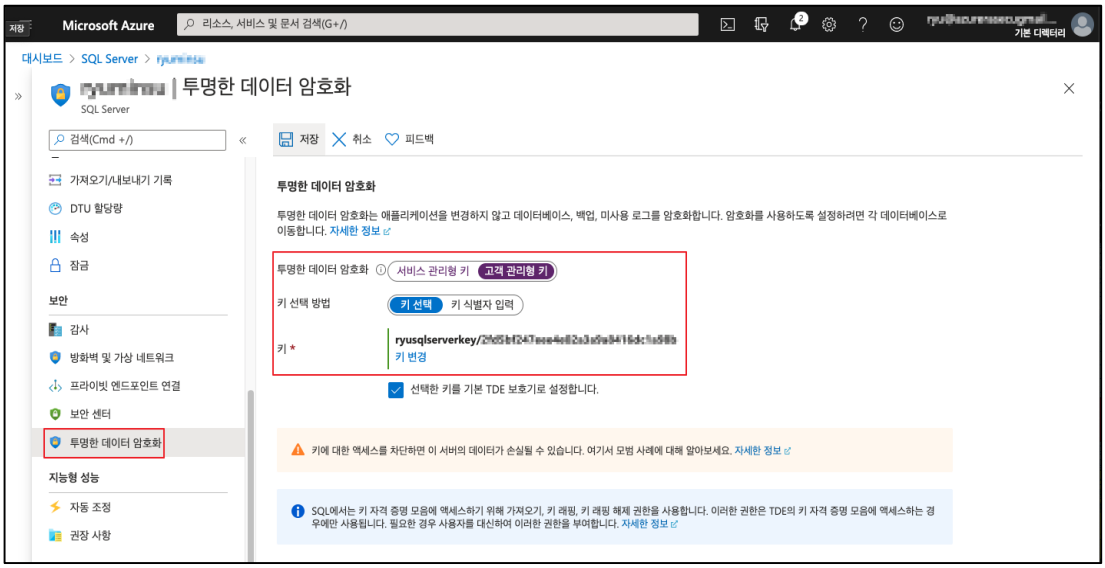
6) Azure key Vault 키 새로 만들기 (암호화 및 만료일자 설정)



7) Azure key Vault 키 선택 완료

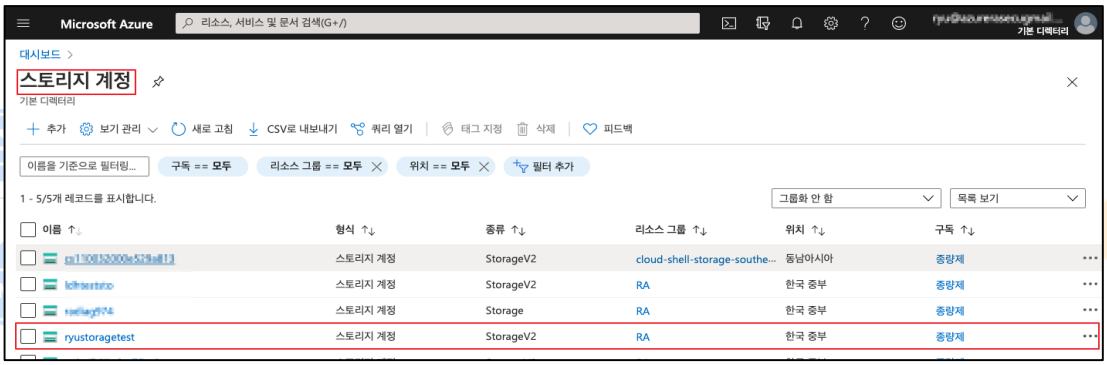


8) 고객 관리형 키로 설정된 투명한 데이터 암호화 설정

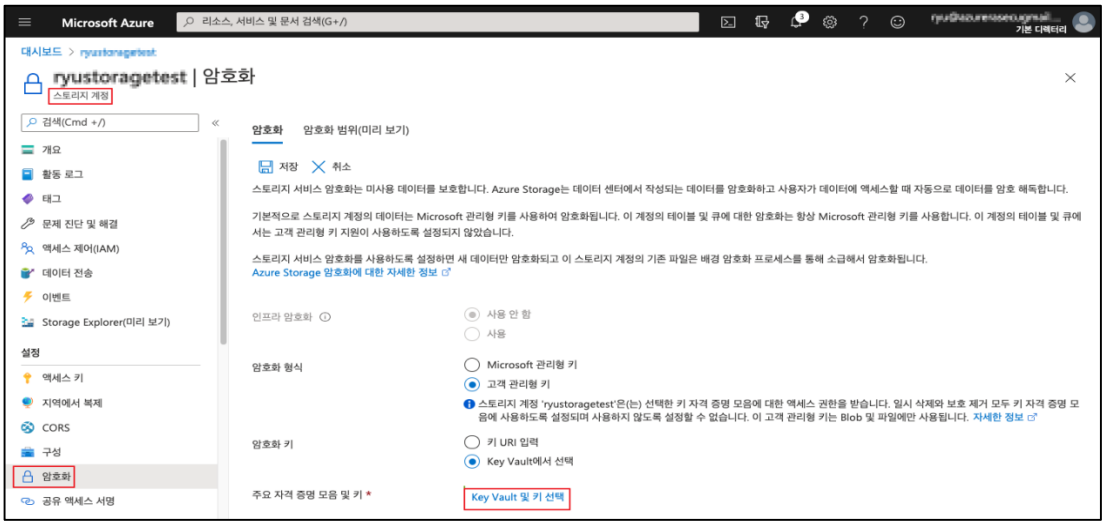


나. 스토리지 계정 암호화 및 만료일자 설정

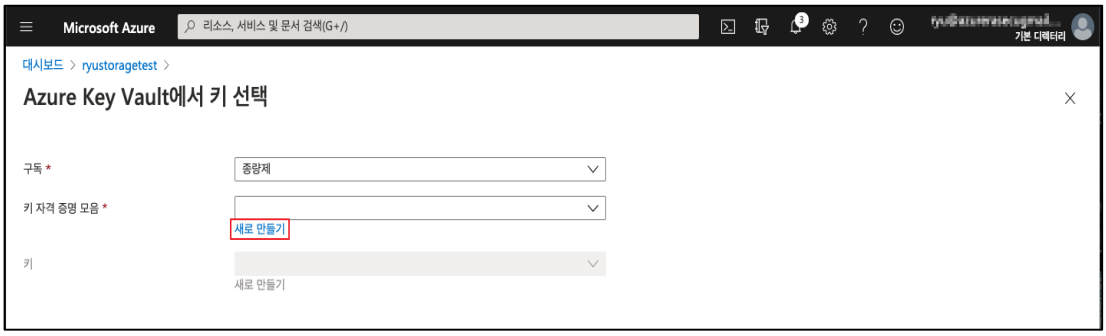
1) 스토리지 계정 선택



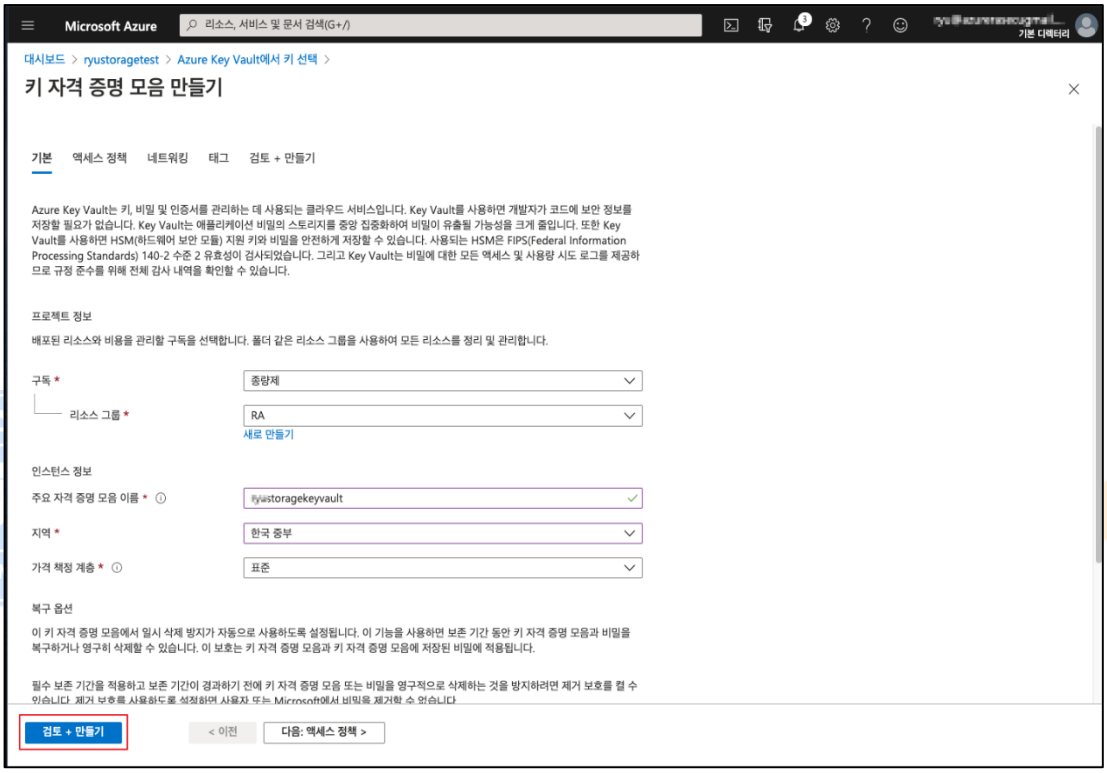
2) 스토리지 계정 암호화 Key Vault 및 키 선택



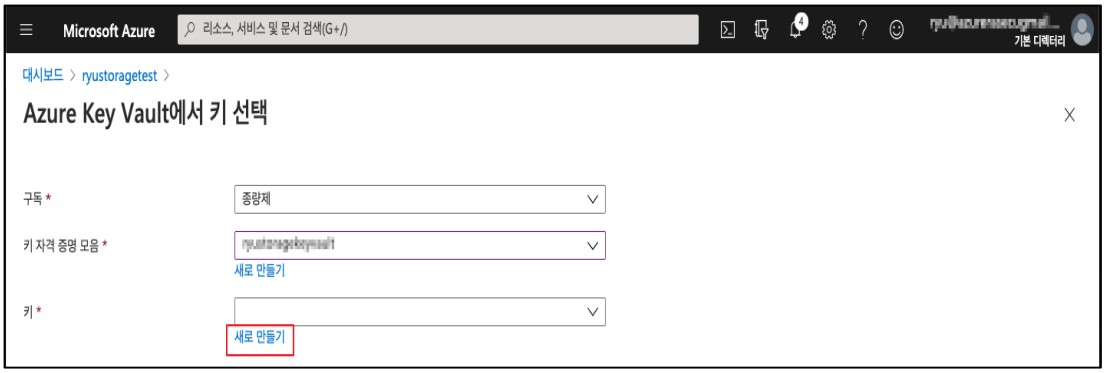
3) Azure Key Vault 키 자격모음 새로 만들기 선택



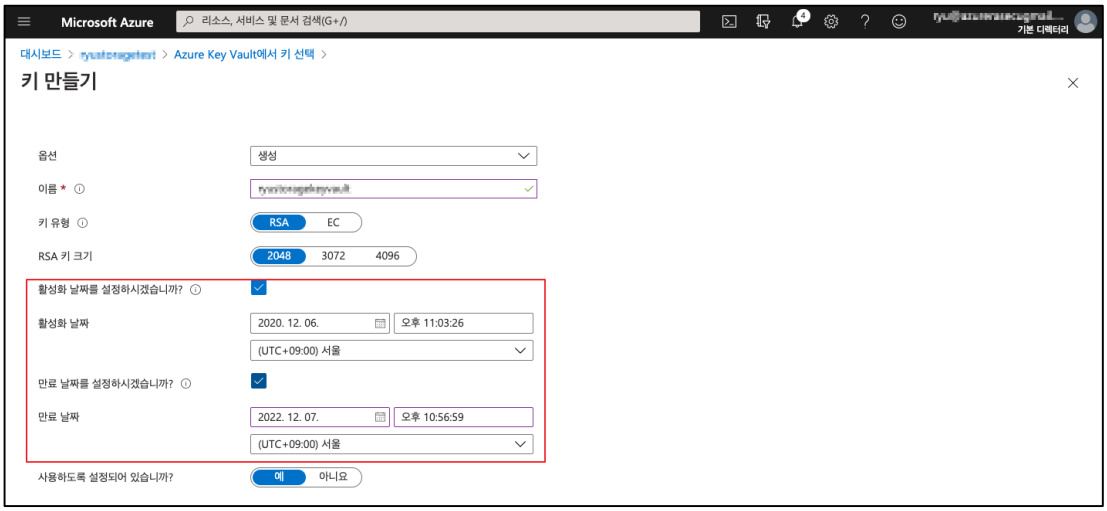
4) Azure Key Vault 키 자격모음 생성



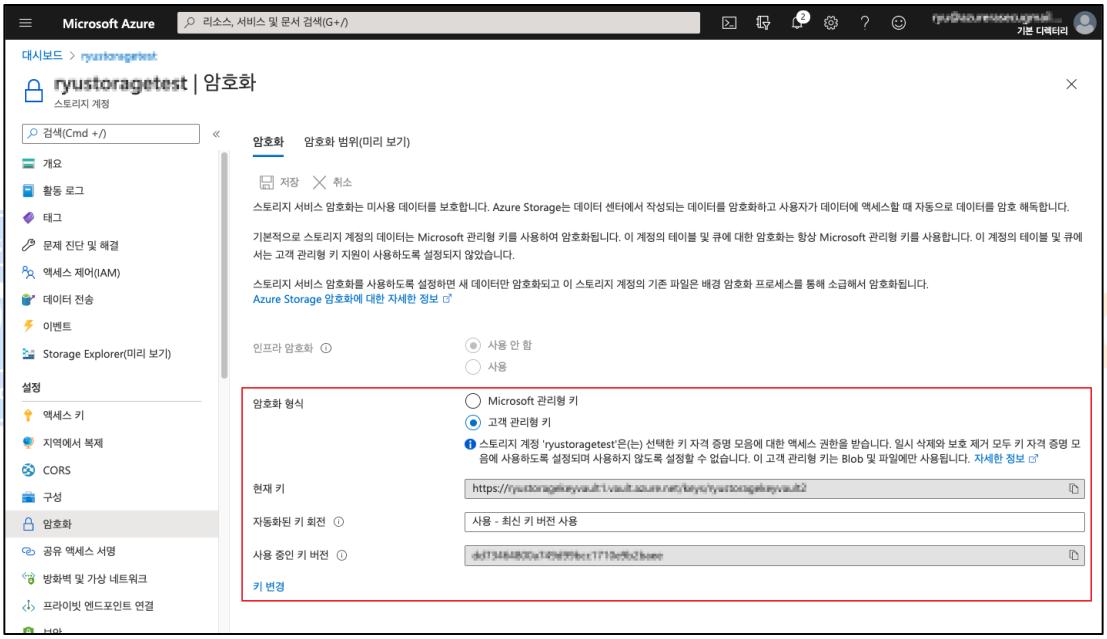
5) Azure Key Vault 키 생성하기



6) 암호화 키 생성 시 암호화 및 만료일자 지정



7) 스토리지 계정 암호화 설정 확인



진단 기준	**양호기준** : 리소스(SQL Server, 스토리지 등) 암호화를 사용자 고유키(Key Vault) 통해 설정하거나 만료일자가 존재 할 경우 **취약기준** : 리소스(SQL Server, 스토리지 등) 암호화에 사용되는 사용자 고유키(Key Vault)의 만료일자가 설정되어 있지 않을 경우
비고	

4. 가상 리소스 관리

4.1 가상 네트워크 디바이스 설정

분류	가상 리소스 관리	중요도	상
항목명	가상 네트워크 디바이스 설정		

항목 설명

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. 이때 가상 네트워크에 연결되는 리소스를 '디바이스'라 표현하며, '연결된 디바이스' 메뉴를 통해 가상 네트워크에 연결되는 Azure 리소스를 확인할 수 있고, 해당 가상 네트워크에 불필요한 디바이스(리소스)를 삭제할 수 있습니다.

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

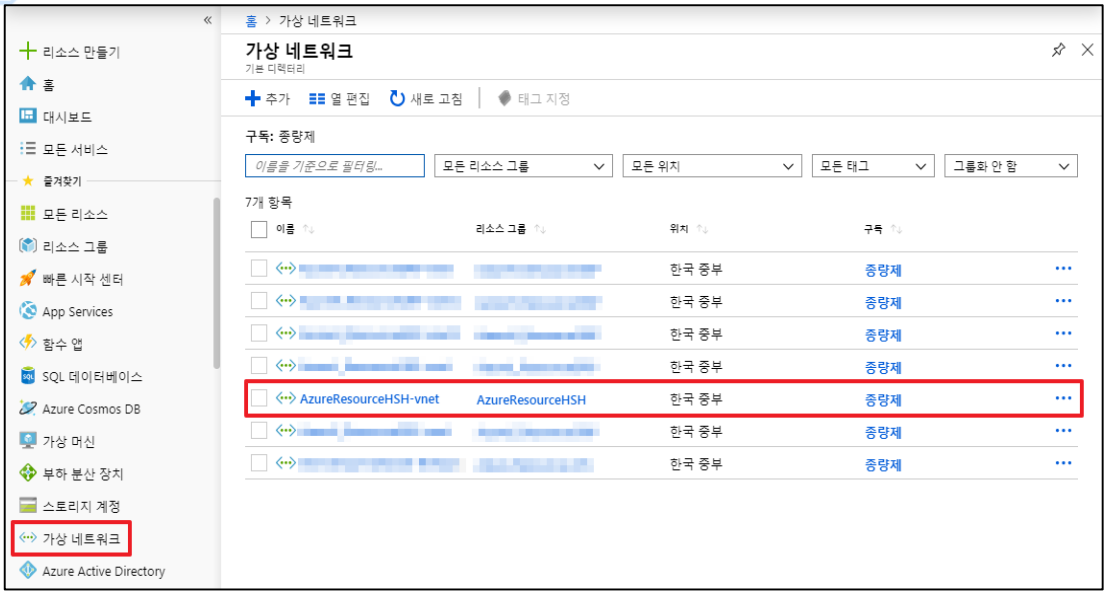
※ 연결된 디바이스 관리 List (예시)

가상 네트워크	연결된 디바이스	서브넷	IP	사용목적	취약 유/무
RsGrpNet001	azurehvm400	ex)dafult_subnet	ex)10.0.0.1	ex)사용목적	N/A
					N/A
					N/A
					N/A
					N/A

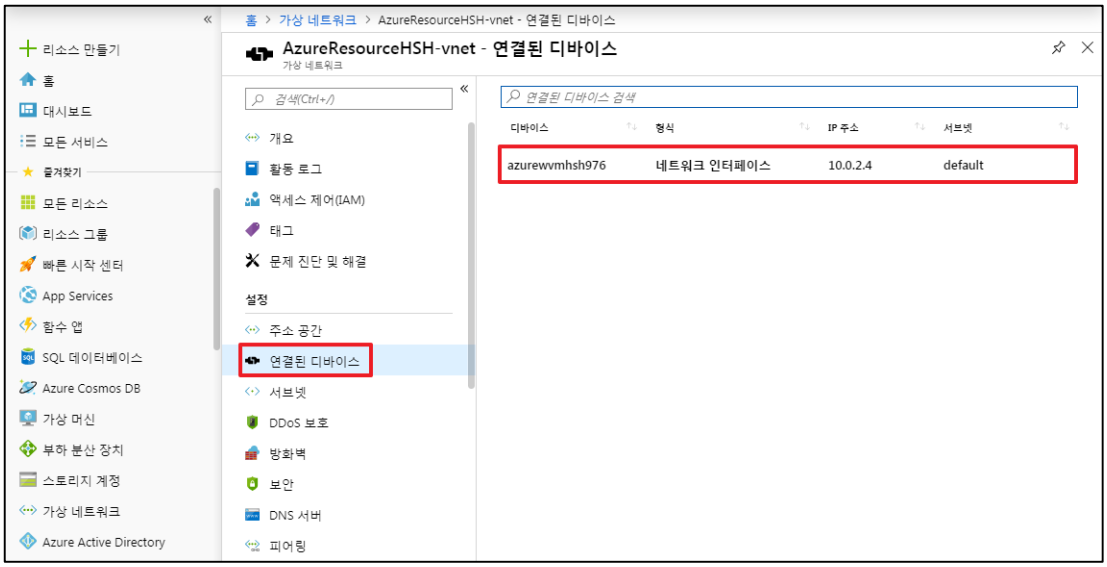
설정 방법

가. 연결된 디바이스 목록 확인 및 삭제 방법

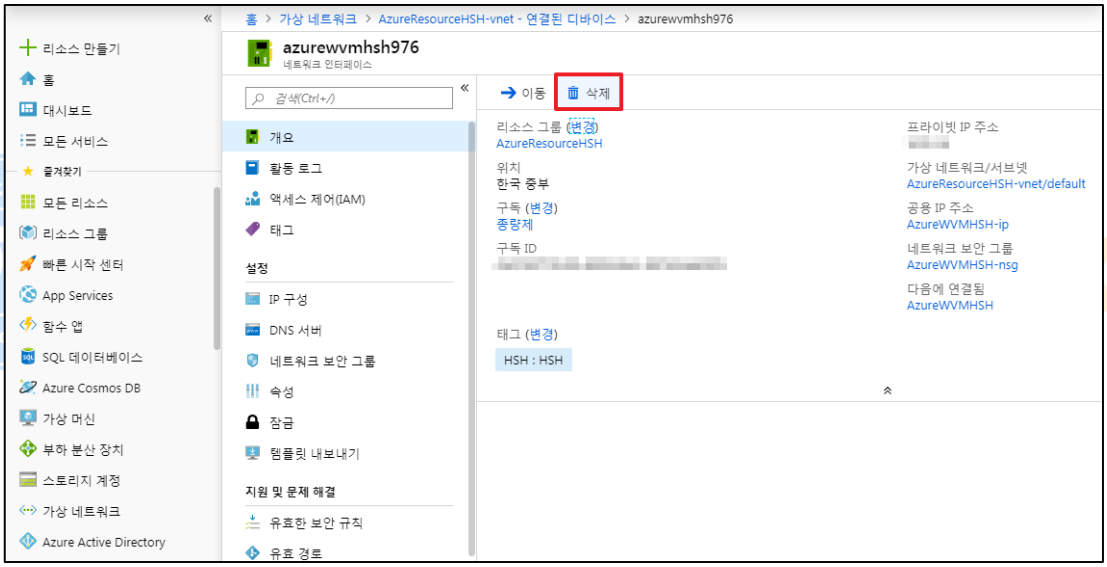
1) 가상 네트워크 메뉴 내 디바이스 목록을 확인할 가상 네트워크 선택



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

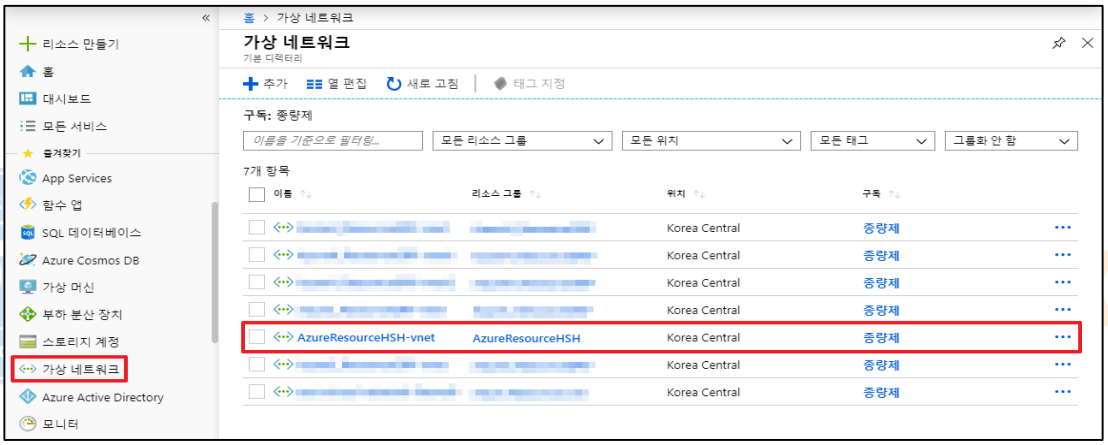
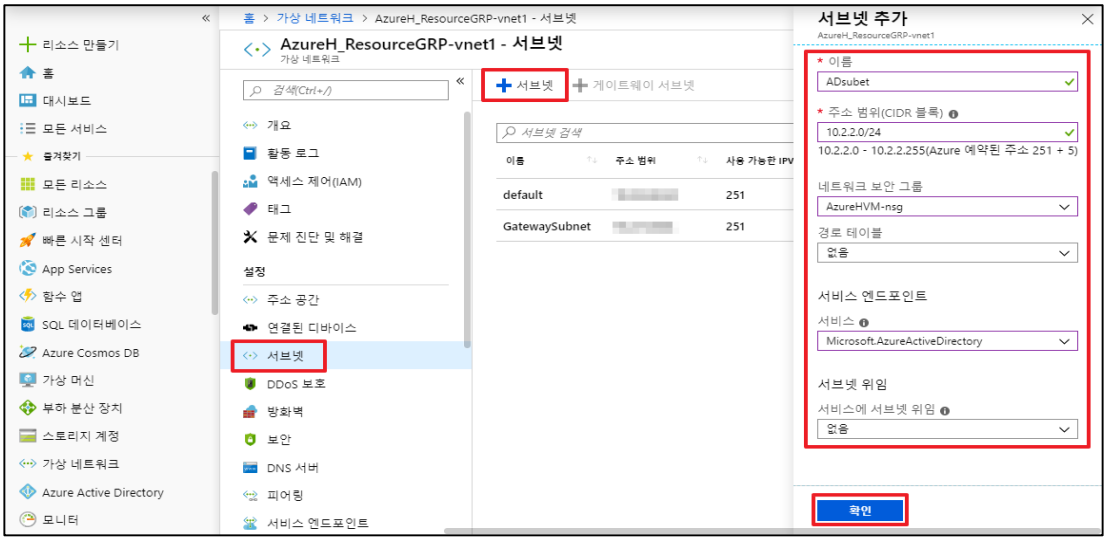


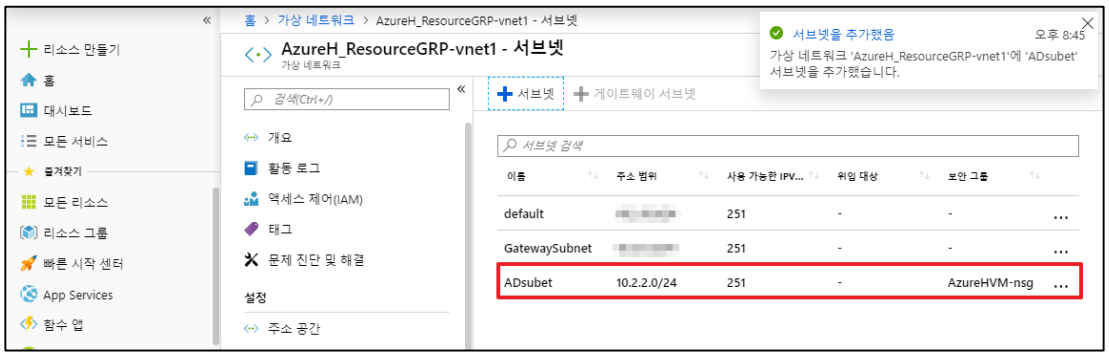
3) 삭제할 디바이스 선택 후 삭제



진단 기준	**양호기준** : 가상 네트워크 사용 목적에 필요한 디바이스만 연결되어 있을 경우 **취약기준** : 가상 네트워크 사용 목적에 필요한 디바이스만 연결되어 있지 않을 경우
비고	

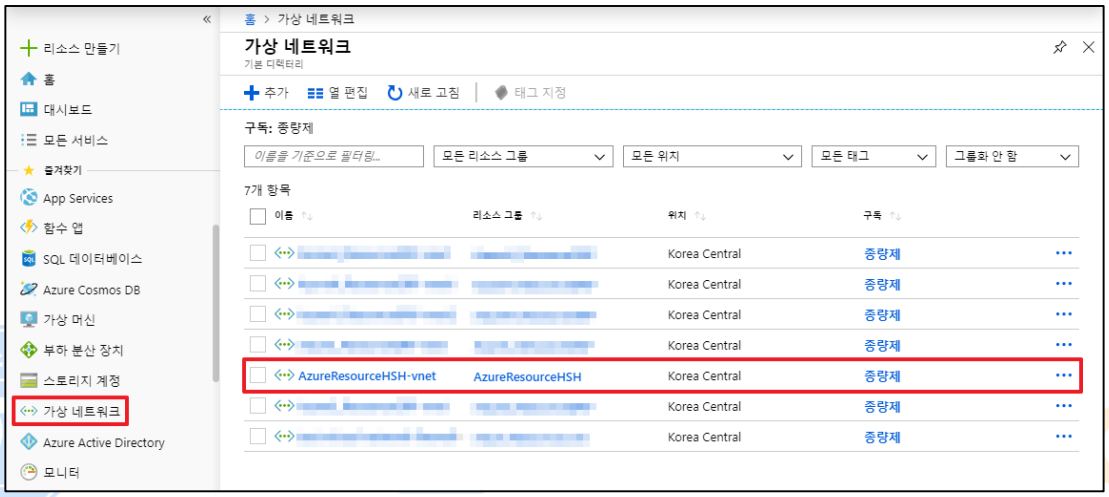
4.2 서브넷 연결 관리

분류	가상 리소스 관리	중요도	하
항목명	서브넷 연결 관리		
항목 설명	가상 네트워크는 하나 또는 여러개의 서브넷으로 이루어져 있으며, 서브넷은 가상 네트워크 내 IP 주소의 범위를 나타냅니다. 같은 가상 네트워크의 서브넷은 단일 Azure 지역으로 범위가 지정되며, 가상 네트워크 피어링을 사용하여 여러 지역의 여러개의 가상 네트워크를 연결할 수 있습니다. 이때, 가상 네트워크에 불필요한 범위의 서브넷으로 구성되어 있을 경우, 보안상 위험이 발생할 수 있으므로 불필요한 서브넷에 대한 관리가 필요합니다. **※ Private 서브넷에 공용IP를 갖는 VM이 연결될 경우, IP직접입력을 통해 외부에서 VM에 접근이 가능하므로, Private 서브넷에 공용IP을 등록하지 않는 것을 권고합니다.**		
설정 방법	**가. 서브넷 추가 설정 방법** 1) 가상 네트워크 메뉴 내 서브넷을 추가할 가상 네트워크 선택  2) 서브넷 메뉴 내 서브넷 추가 버튼 클릭 및 서브넷 설정  3) 서브넷 목록 내 추가된 서브넷 정상 생성유무 확인		

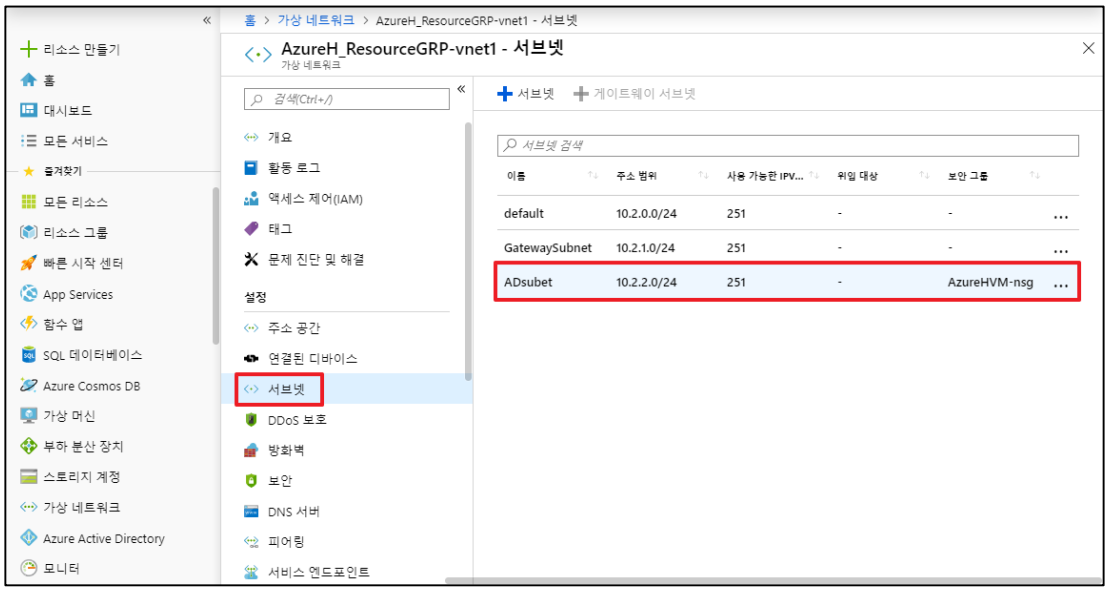


나. 서브넷 확인 및 삭제 방법

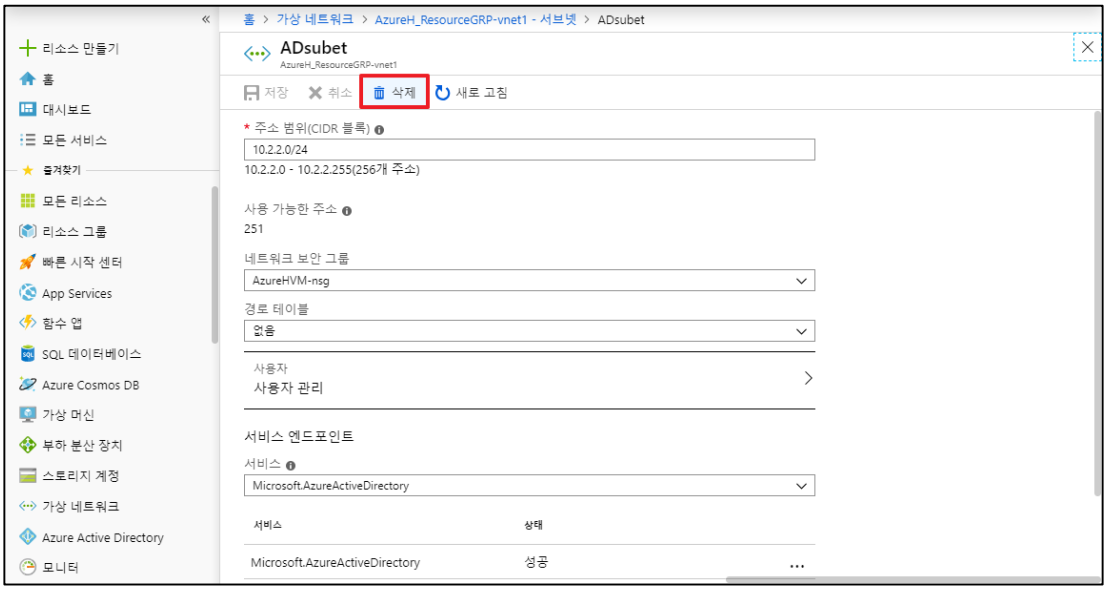
1) 가상 네트워크 메뉴 내 서브넷을 확인할 가상 네트워크 선택



2) 서브넷 메뉴 내 불필요하거나 알 수 없는 서브넷 존재유무 확인

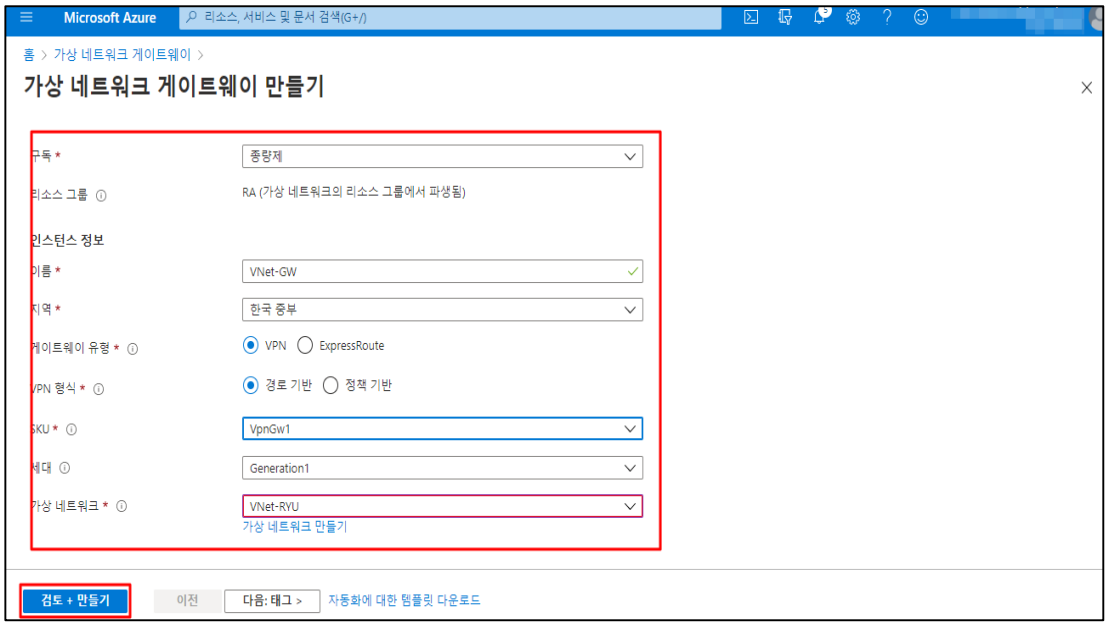


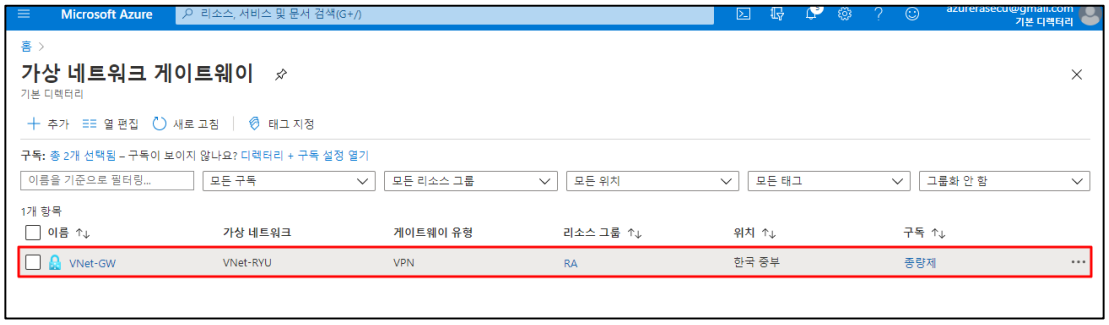
3) 서브넷 선택 후 삭제

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: 서브넷에 인가된 네트워크 보안 그룹 및 서비스 엔드포인트만 연결되어 있는 경우

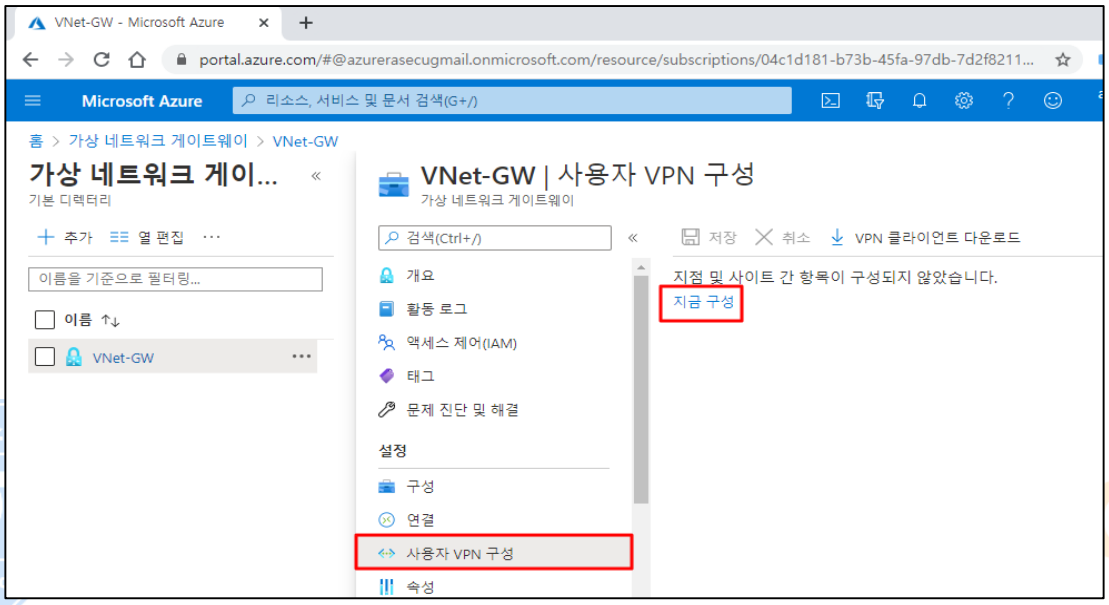
취약기준
: 서브넷에 인가된 네트워크 보안 그룹 및 서비스 엔드포인트만 연결되어 있지 않을 경우</td></tr>
<tr><td>비고</td><td>사용하고 있는 서비스가 대외적으로 Open해도 영향도가 없을 경우에는 예외사항으로 함</td></tr>
</table>

4.3 내부 가상 네트워크 보안관리

분류	가상 리소스 관리	중요도	상
항목명	내부 가상 네트워크 보안관리		
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 고가용성과 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		

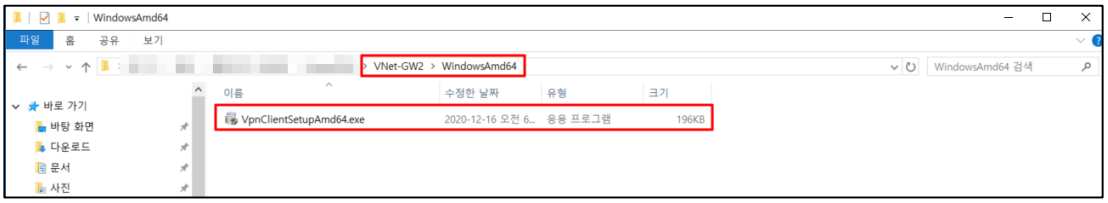


4) 사용자 VPN 구성

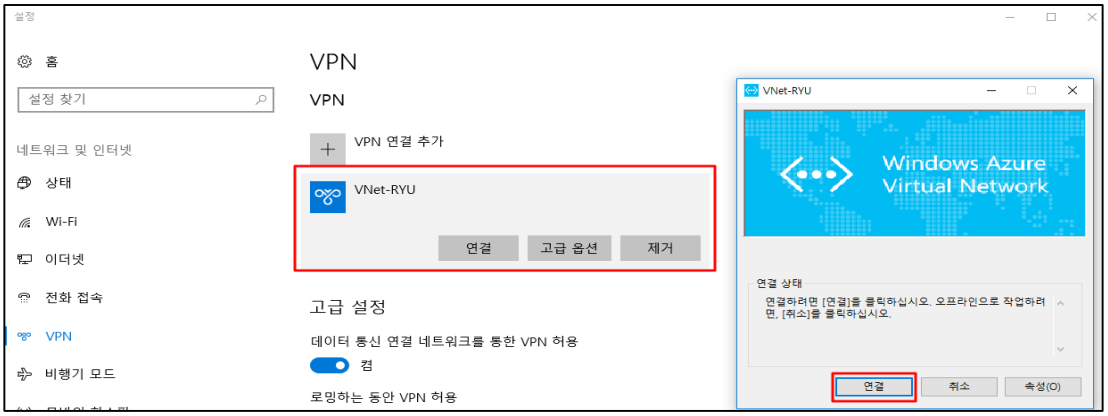


5) VPN 정보 입력, 인증서 등록 및 VPN 클라이언트 다운로드

6) VPN 클라이언트 설치



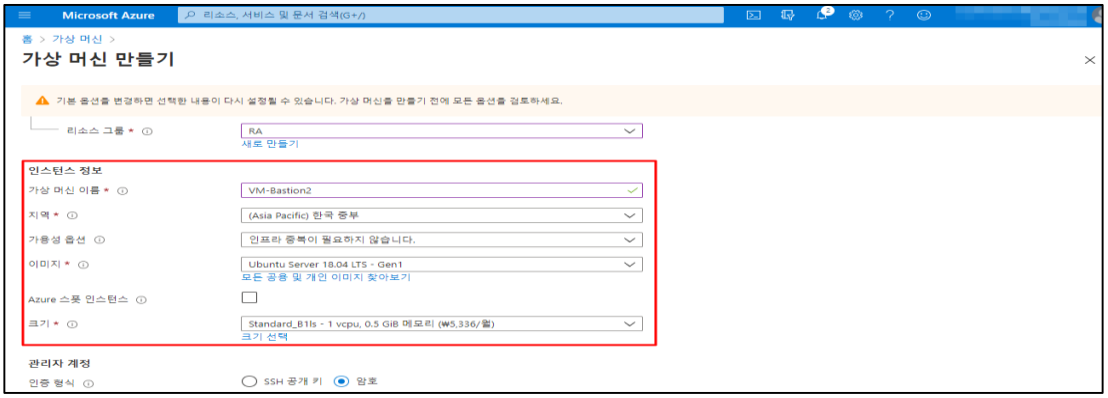
7) 로컬에서 설치된 VPN 연결 시도



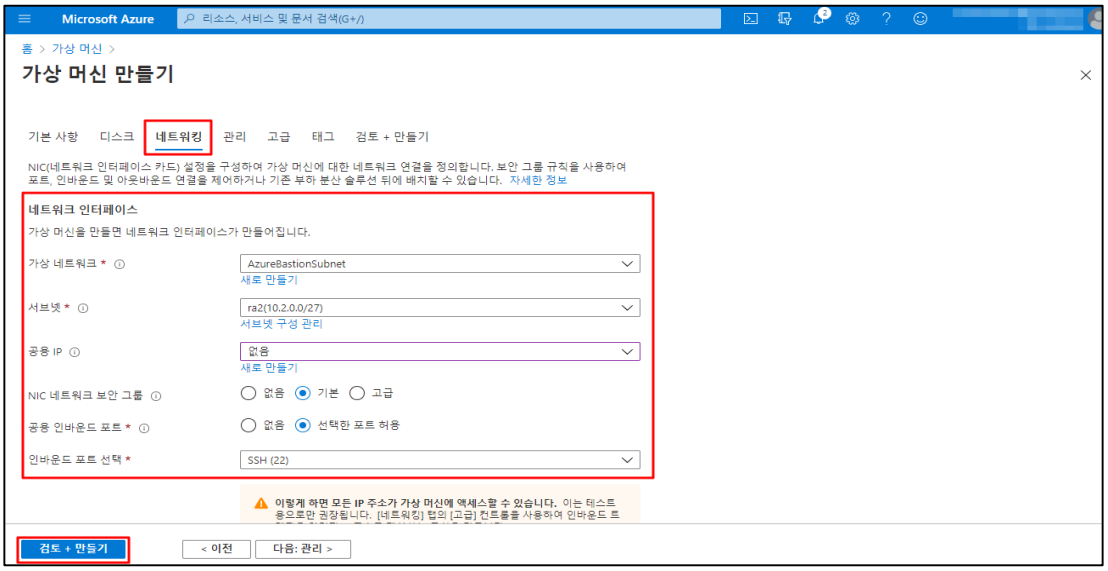
8) VPN 구성 시 설정한 주소 풀 IP 정보 확인

나. Bastion 가상 머신 이용한 연결

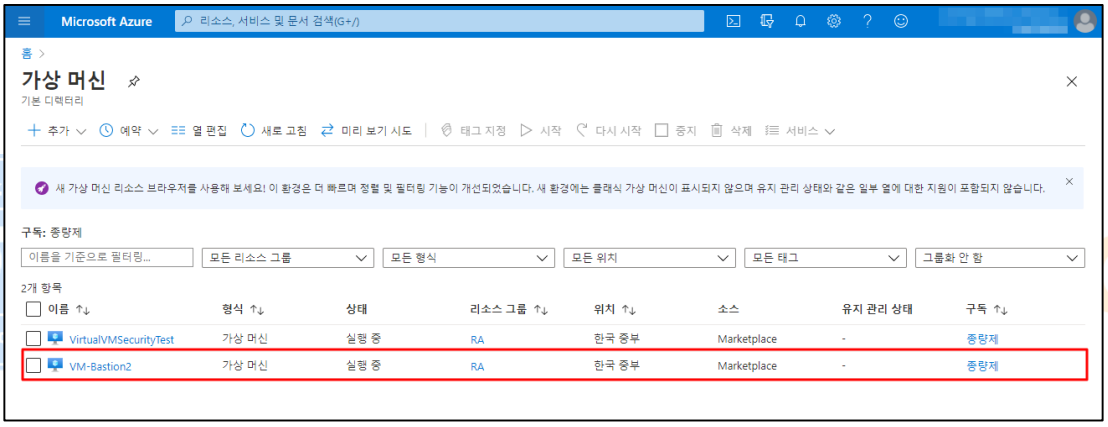
1) Bastion에 포함될 가상 머신 추가



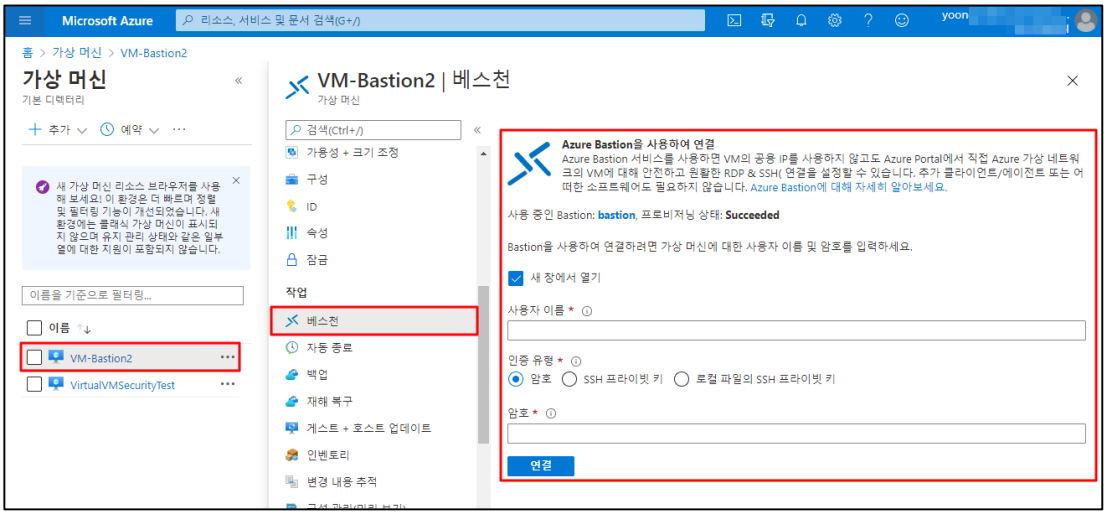
2) Bastion에 포함될 가상 네트워크 등록



3) 생성된 가상 머신 확인



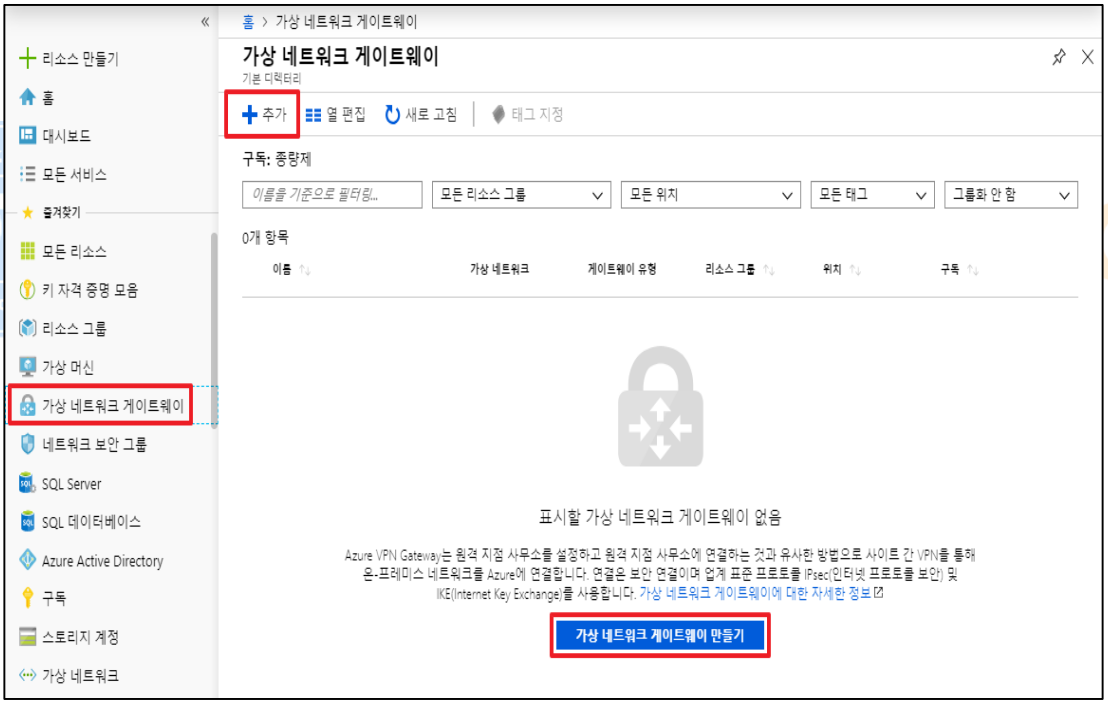
4) 가상 머신 내 Bastion 메뉴를 통해 연결 확인

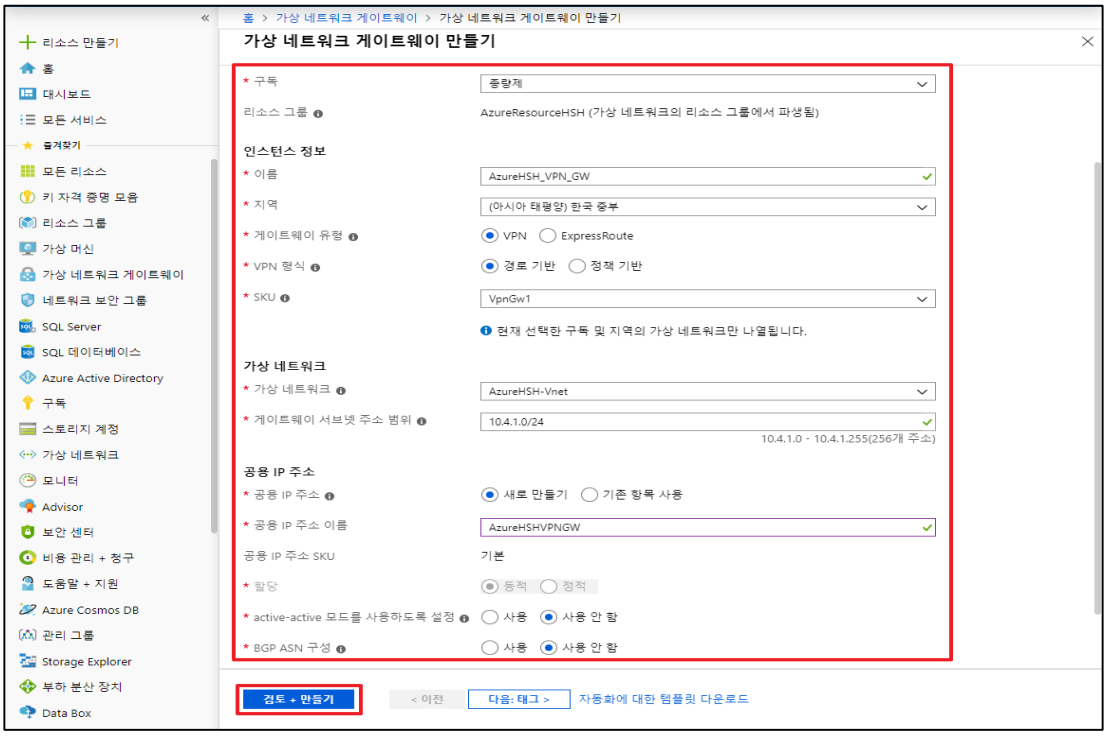


진단 기준	**양호기준** : 내부 서비스를 제공하는 가상네트워크에 VPN Gateway 및 Bastion 가상머신을 사용하고 있을

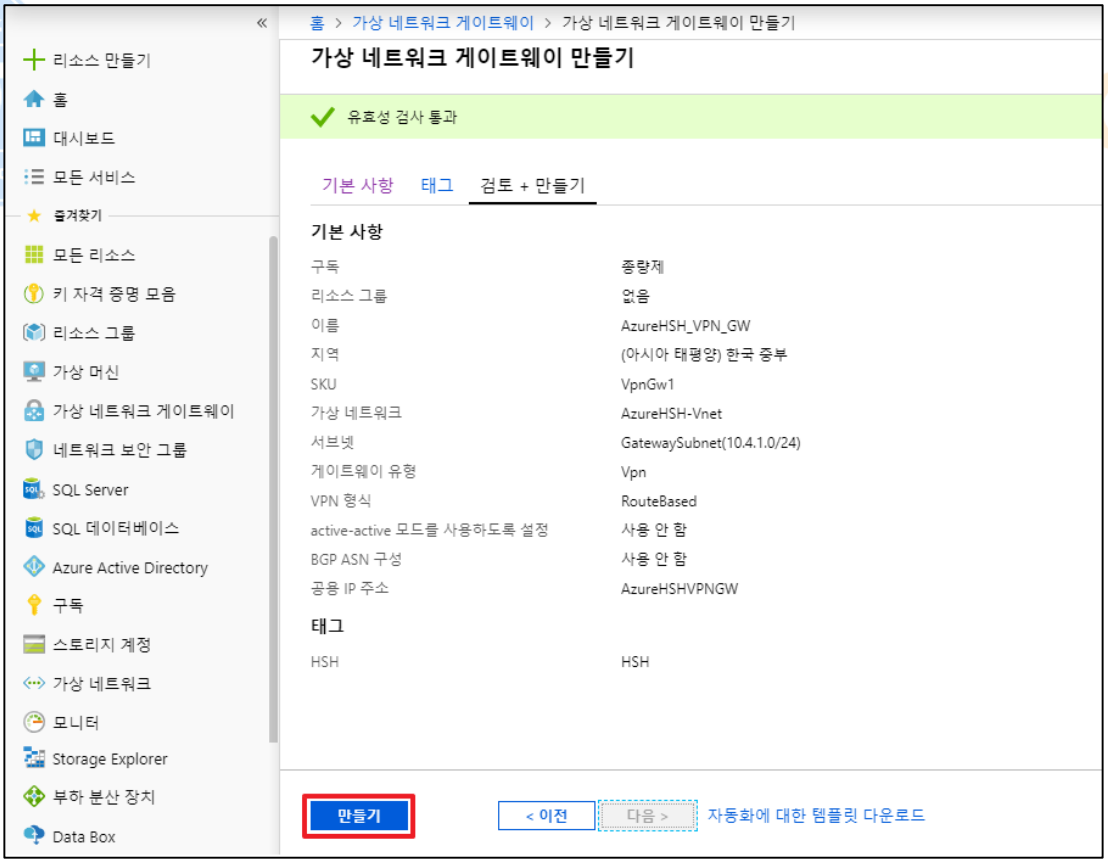
	경우 **취약기준** : 내부 서비스를 제공하는 가상네트워크에 VPN Gateway 및 Bastion 가상머신을 사용하고 있지 않을 경우
비고	

4.4 가상 네트워크 게이트웨이 연결 관리

분류	가상 리소스 관리	중요도	상
항목명	가상 네트워크 게이트웨이 연결 관리		
항목 설명	VPN Gateway는 공용 인터넷을 통해 Azure 가상 네트워크와 온-프레미스 위치 간에 암호화된 트래픽을 전송하는 데 사용되는 특정 유형의 가상 네트워크 게이트웨이입니다. VPN Gateway를 사용하여 Microsoft 네트워크를 통해 Azure 가상 네트워크 간에 암호화된 트래픽을 보낼 수도 있습니다. VPN Gateway는 각 가상 네트워크당 하나만 사용할 수 있습니다. 그러나 동일한 VPN Gateway에 대해 여러 연결을 만들 수 있습니다. 동일한 VPN Gateway에 대해 여러 연결을 만들면 모든 VPN 터널이 사용 가능한 게이트웨이 대역폭을 공유합니다. VPN Gateway에 연결된 네트워크 내 공용 IP를 할당받은 리소스가 존재할 경우 AZURE 리소스에 비정상적인 접근 또는 2차 공격에 활용될 수 있습니다.		
설정 방법	**가. 가상 네트워크 게이트웨이 생성 방법** 1) 가상 네트워크 메뉴 내 추가 버튼 및 가상 네트워크 게이트웨이 만들기 선택  2) 가상 네트워크 게이트웨이 값 설정		



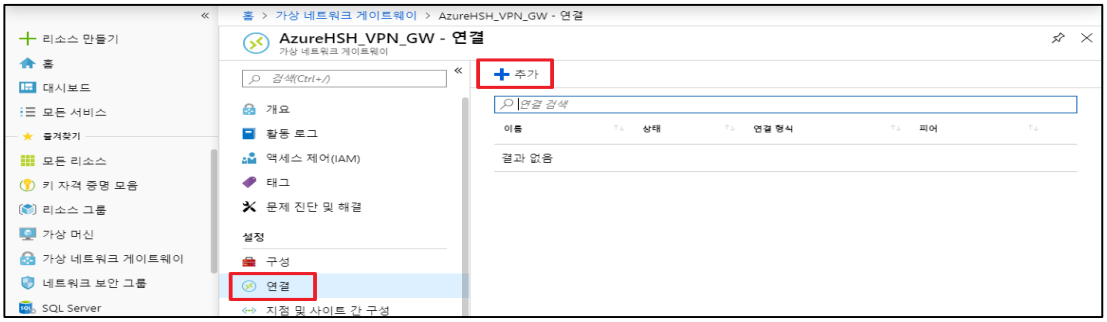
3) 설정된 값 검토 및 만들기



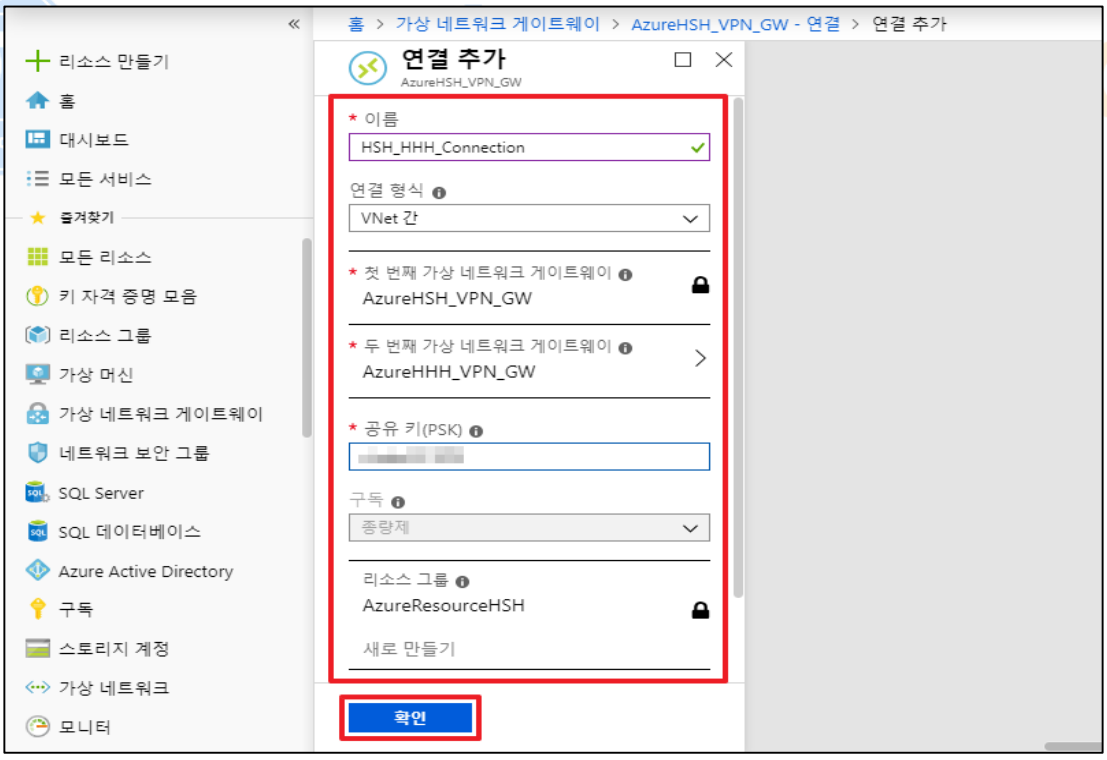
나. 가상 네트워크 게이트웨이 상호간 연결 방법

1) 가상 네트워크 메뉴 내 연결을 설정할 첫 번째 가상 네트워크 게이트웨이 선택

2) 연결 메뉴 내 추가 버튼 클릭

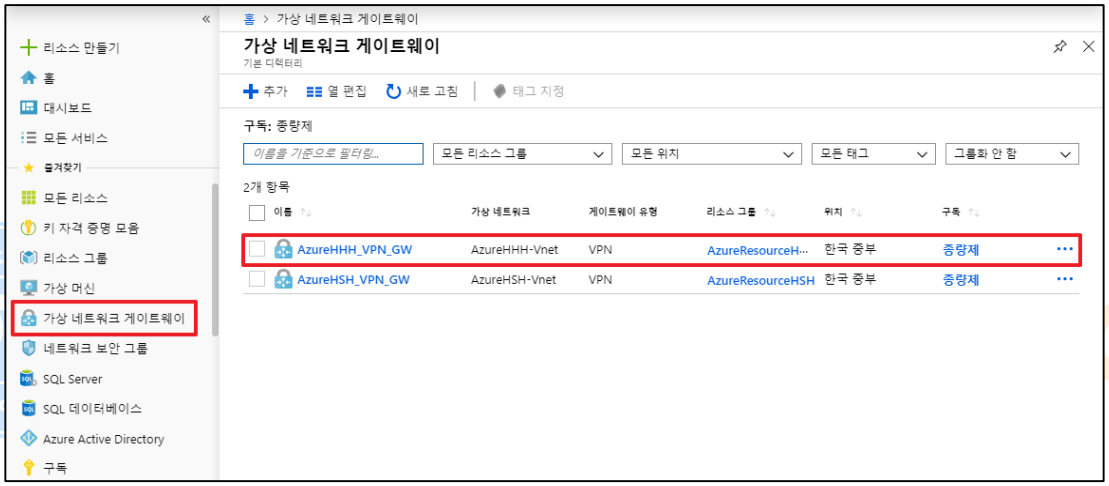


3) 연결 추가 값 설정 및 확인 (공유키의 경우 두 번째 가상 네트워크 게이트웨이 설정 시 필요)



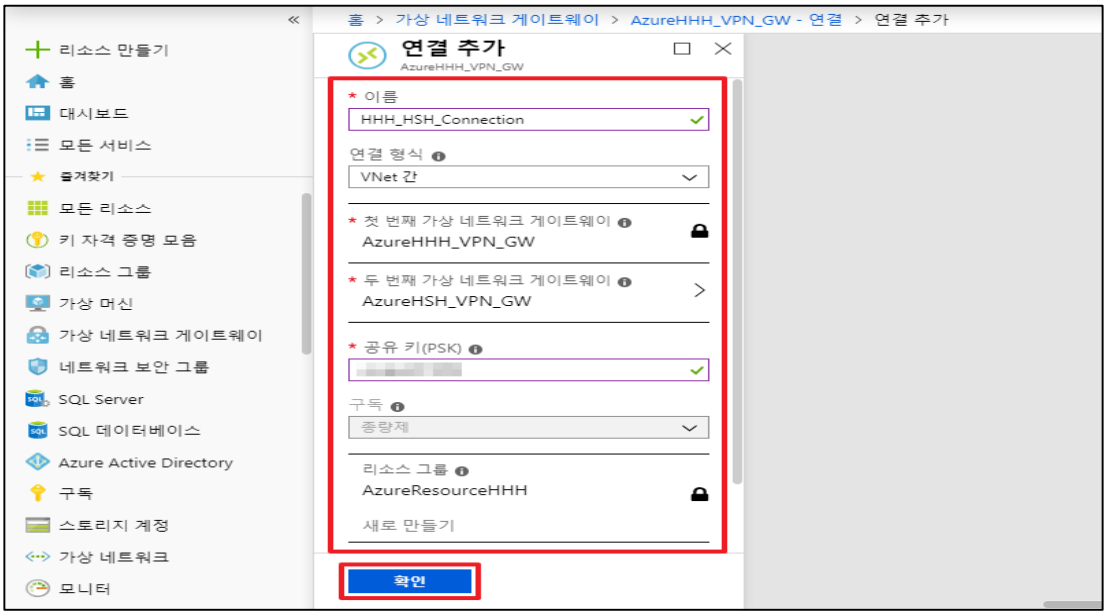
4) 연결 설정 상태 값 확인 (상호간 연결 설정이 안됐기 때문에 '알 수 없음' 으로 됨)

5) 가상 네트워크 메뉴 내 연결을 설정할 두 번째 가상 네트워크 게이트웨이 선택

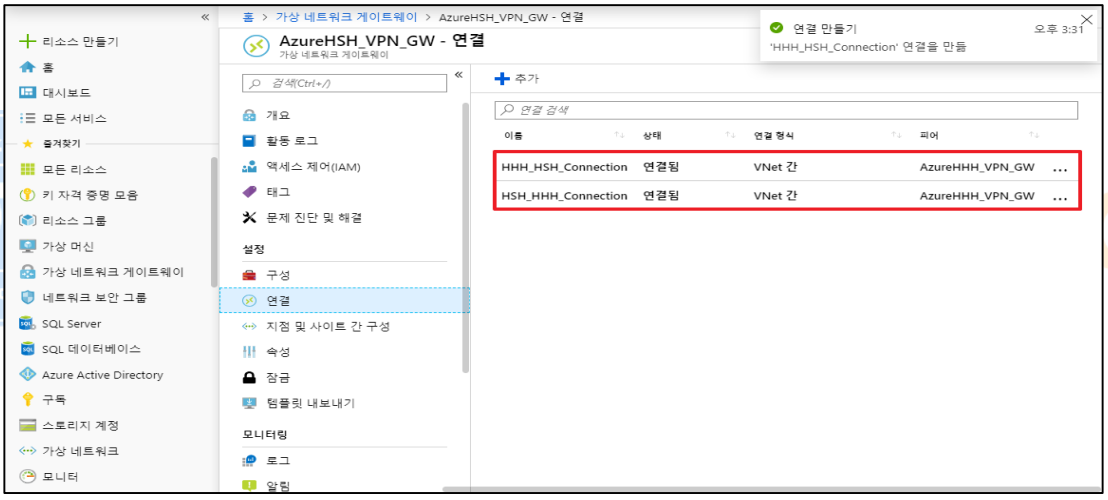


6) 연결 메뉴 내 추가 버튼 클릭

7) 연결 추가 값 설정 및 확인 (공유키의 경우 첫 번째 가상 네트워크 게이트웨이 설정 값과 동일)

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


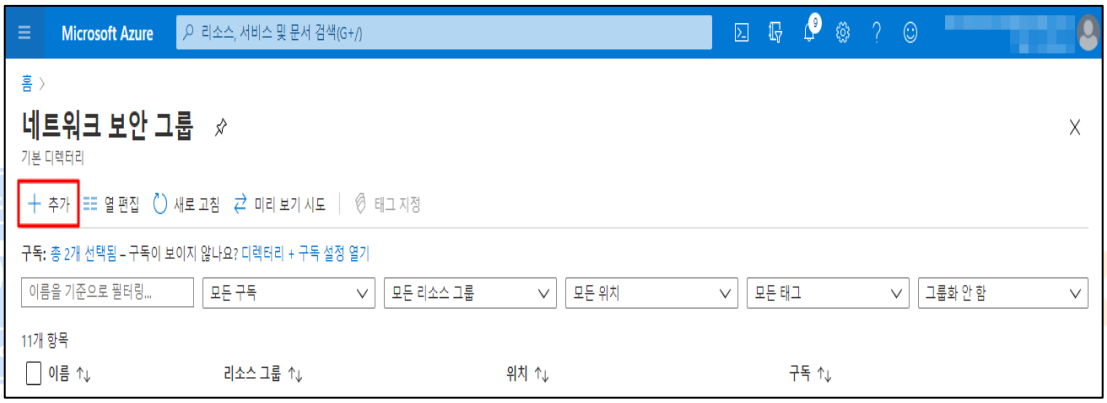
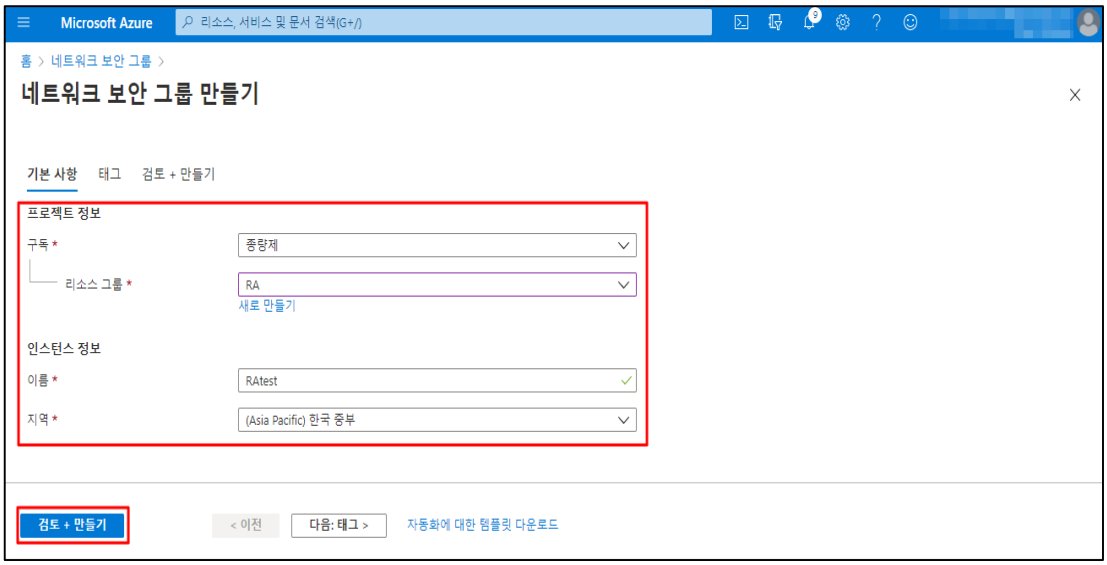
8) 정상적으로 설정되었는지 확인

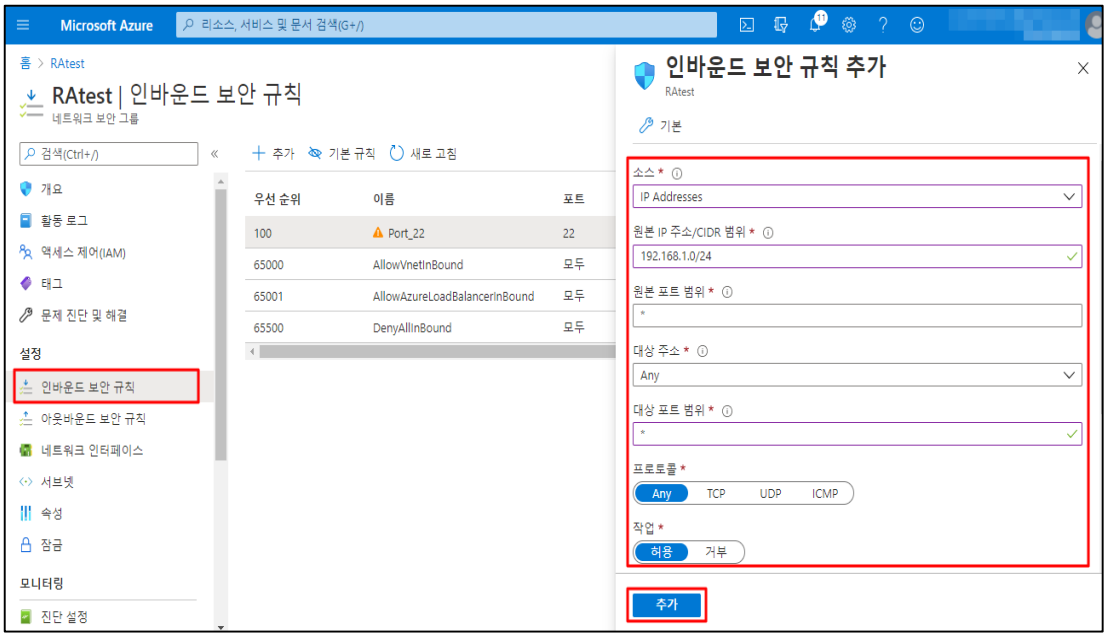


</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: VPN Gateway 연결된 대상 네트워크 내 공용IP를 할당 받은 리소스가 존재하고 있지 않을 경우

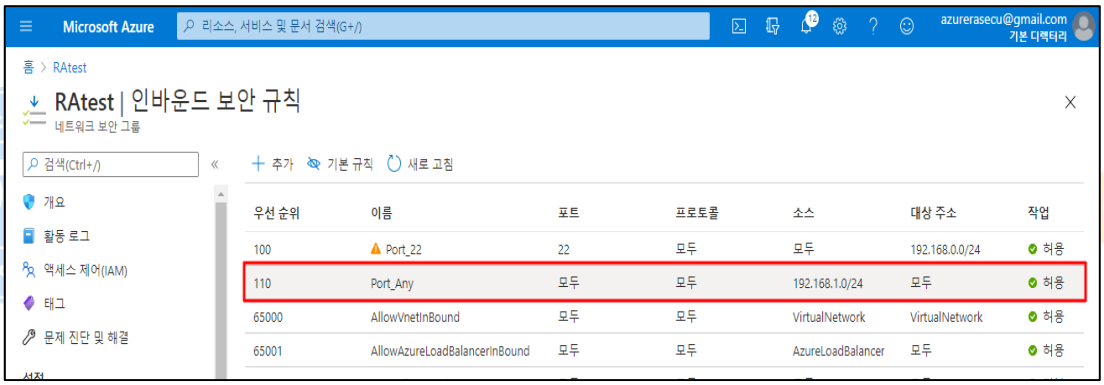
취약기준
: VPN Gateway 연결된 대상 네트워크 내 공용IP를 할당 받은 리소스가 존재하고 있을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

4.5 보안그룹 인/아웃바운드 ANY 설정 관리

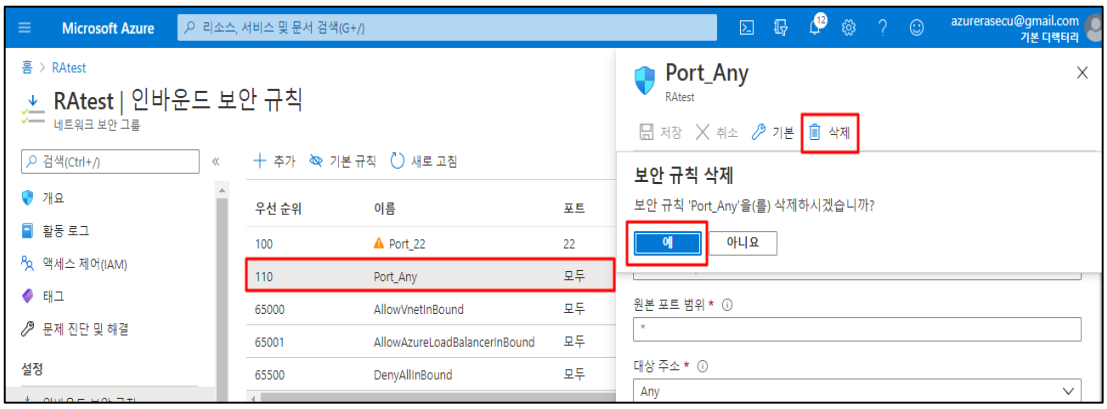
분류	가상 리소스 관리	중요도	상
항목명	보안그룹 인/아웃바운드 ANY 설정 관리		
항목 설명	네트워크 보안 그룹 (Security Group)은 가상머신에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할로서 네트워크 리소스에서 가상머신을 시작할 때 서브넷 수준이 아니라 가상머신 수준에서 작동하므로 네트워크 리소스에 있는 서브넷의 각 가상머신을 서로 다른 보안 그룹 세트에 할당할 수 있습니다. 보안그룹은 네트워크 리소스 별 규칙을 추가하거나 제거가 가능하며 인바운드 트래픽(수신)이나 아웃바운드 트래픽(송신)에 적용되므로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



2) Port가 ANY인 규칙 확인

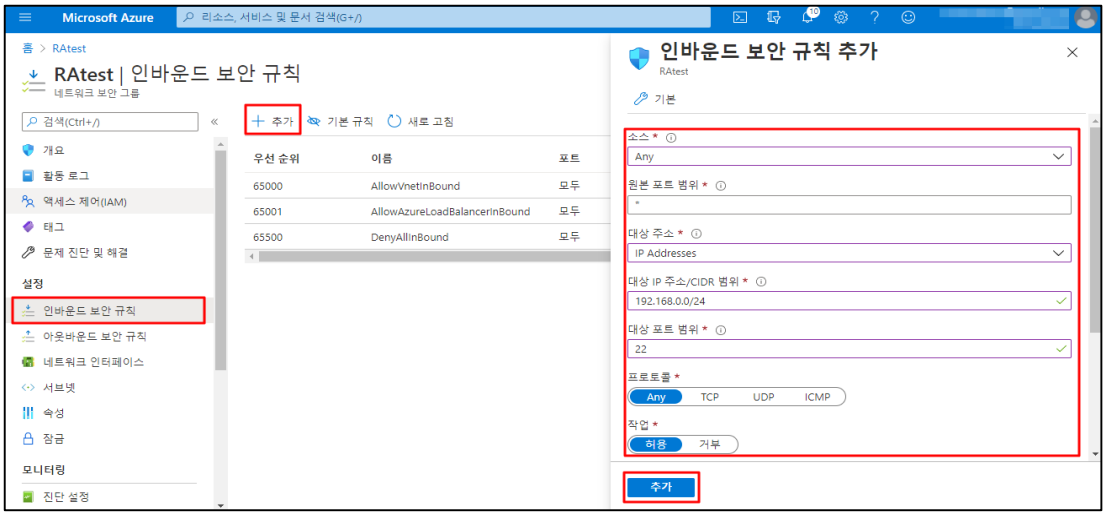


3) 인/아웃바운드 규칙 내 불필요하게 Any로 허용된 Port 삭제

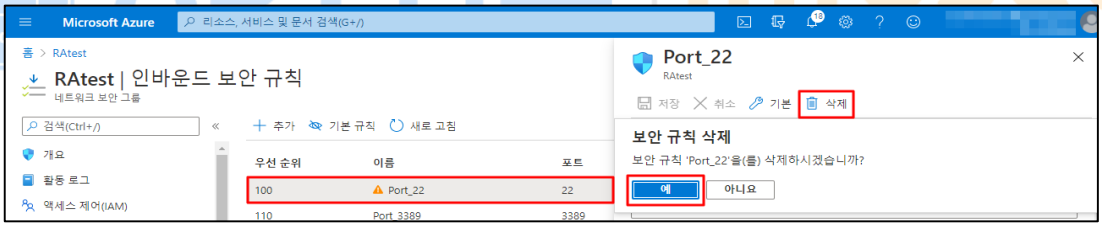


다. 네트워크 보안 그룹 IP Address 설정

1) 인/아웃바운드 규칙 추가

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


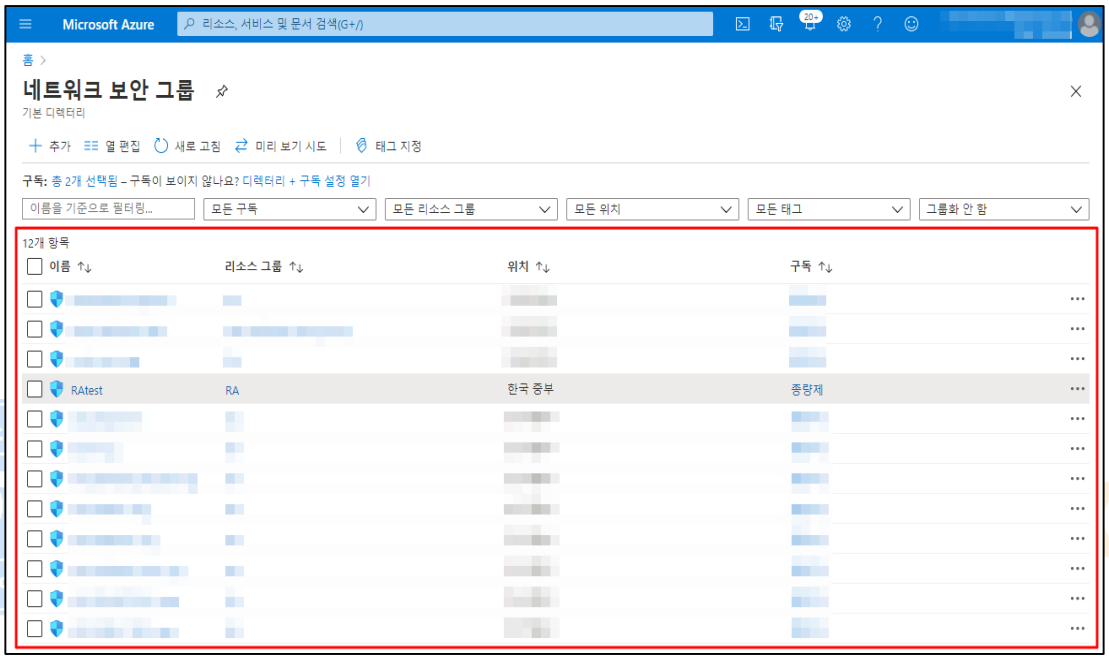
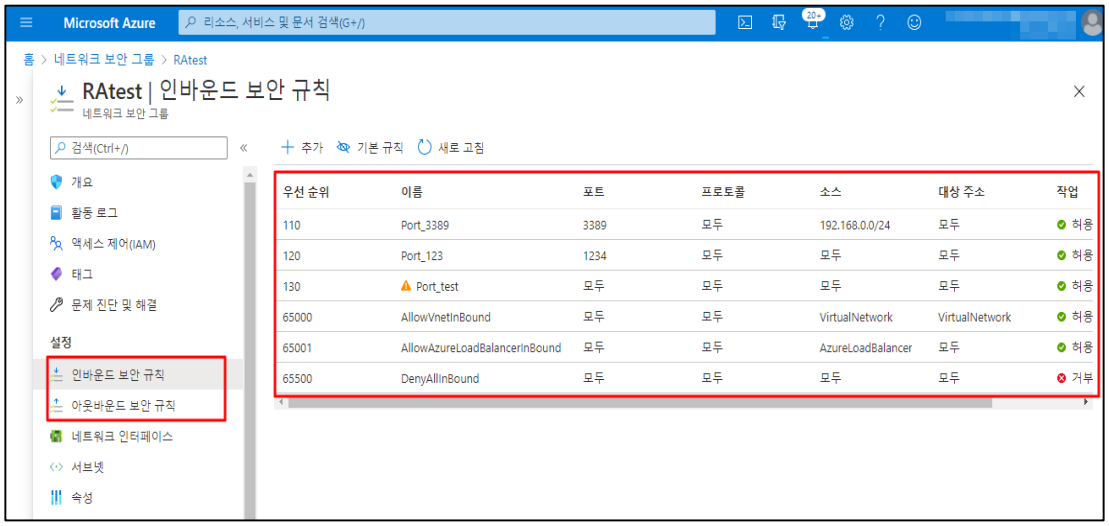
2) Source 또는 Destination 설정이 Any인 규칙 확인

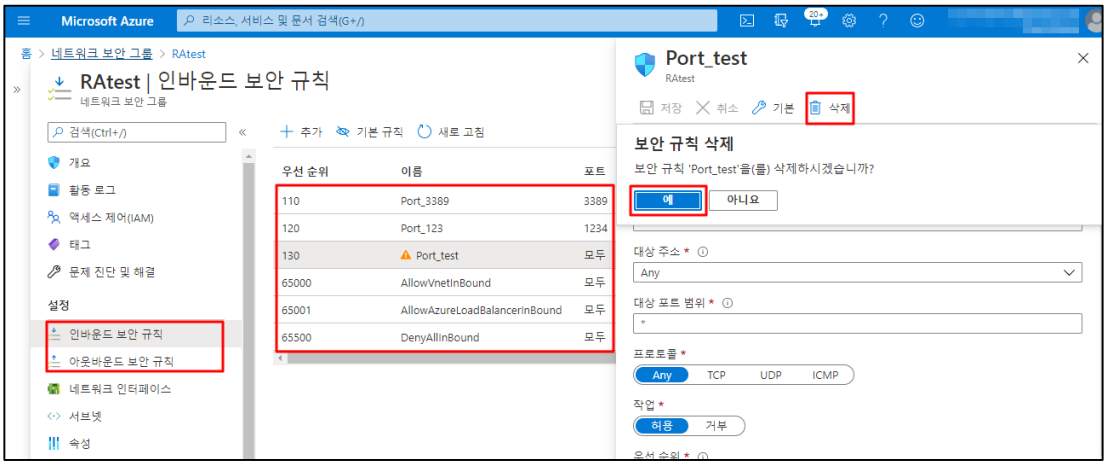

3) 불필요한 규칙 삭제


</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 인/아웃바운드 규칙 내 모든 서비스를 Any(IP, Port 등)로 허용하는 정책이 존재하고 있지 않을 경우

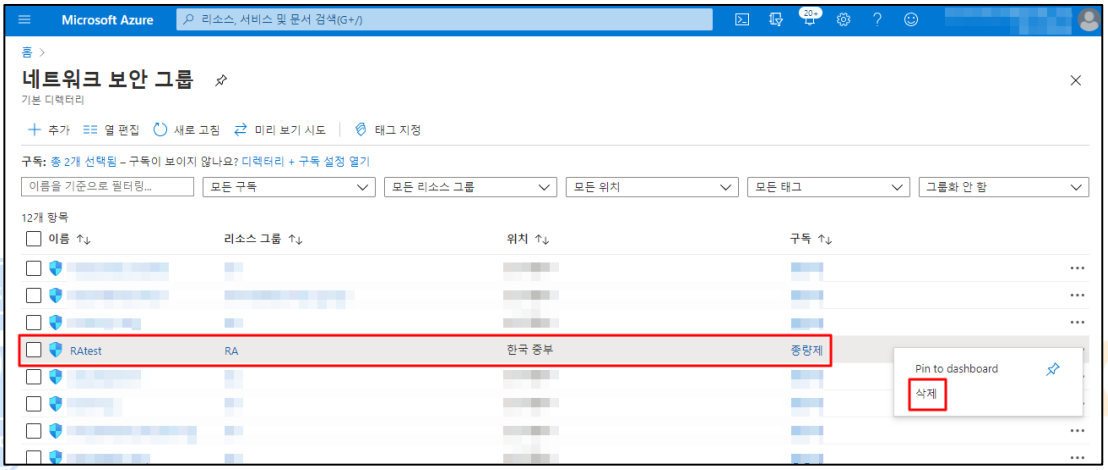
취약기준
: 인/아웃바운드 규칙 내 모든 서비스를 Any(IP, Port 등)로 허용하는 정책이 존재하고 있을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

4.6 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 리소스 별 Port 규칙을 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 및 인/아웃바운드 규칙을 확인하여 불필요한 정책 삭제** 1) 네트워크 보안 그룹 리스트 확인  2) 인/아웃바운드 규칙 리스트 확인  3) 불필요한 인/아웃바운드 규칙 삭제		

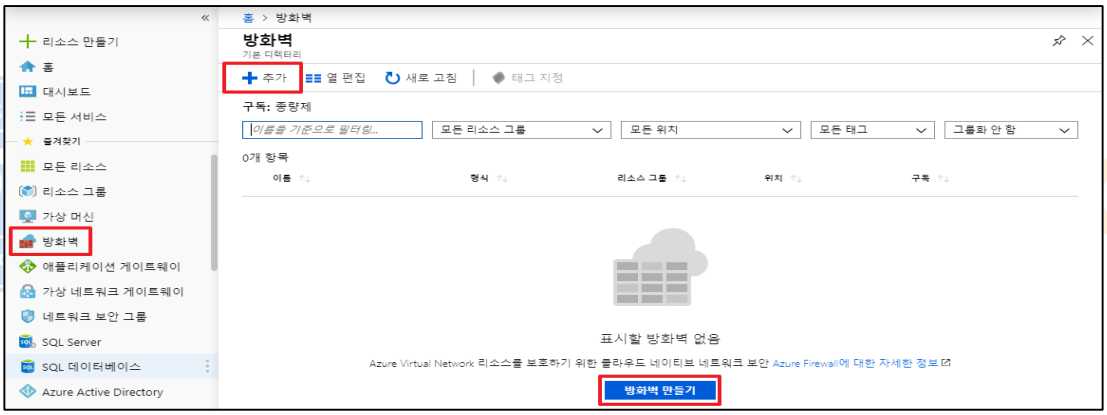
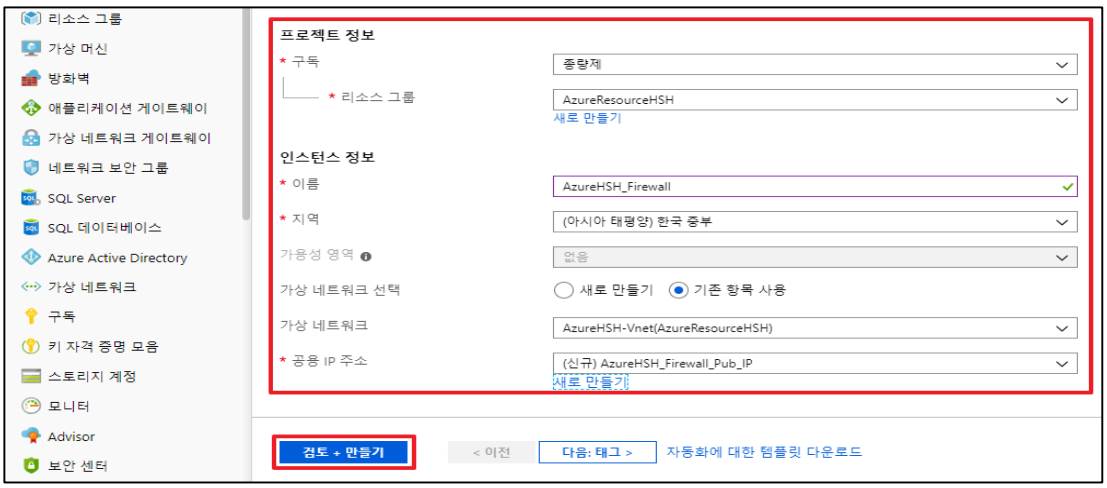


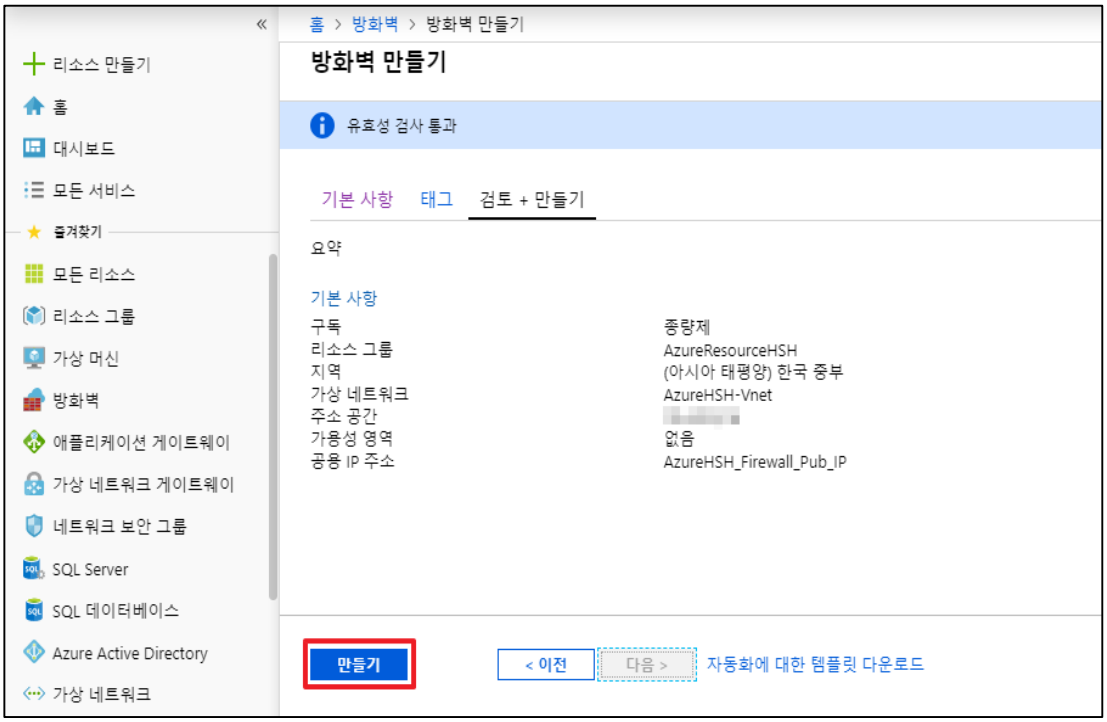
4) 불필요한 네트워크 보안 그룹 삭제



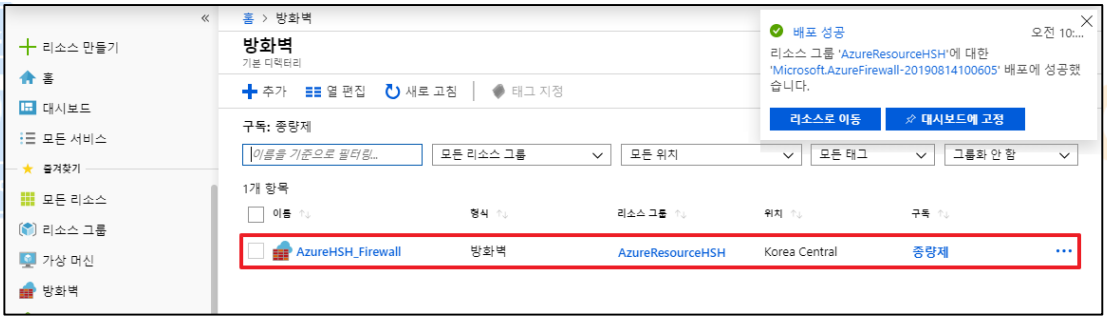
진단 기준	**양호기준** : 인/아웃바운드 규칙 내 서비스 목적을 알 수 없는 정책이 존재하고 있지 않을 경우 **취약기준** : 인/아웃바운드 규칙 내 서비스 목적을 알 수 없는 정책이 존재하고 있을 경우
비고	

4.7 방화벽 인/아웃바운드 ANY 설정 관리

분류	가상 리소스 관리	중요도	상
항목명	방화벽 인/아웃바운드 ANY 설정 관리		
항목 설명	Azure Firewall은 Azure Virtual Network 리소스를 보호하는 관리되는 클라우드 기반 네트워크 보안 서비스입니다. 고가용성 및 무제한 클라우드 확장성이 내장되어 있는 서비스 형태의 완전한 상태 저장 방화벽입니다. 인/아웃바운드 트래픽 내 불필요한 정책이 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 정책이 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 방화벽 추가 및 만들기 버튼 선택  2) 방화벽 관련 값 설정  3) 방화벽 값 검토 및 만들기		



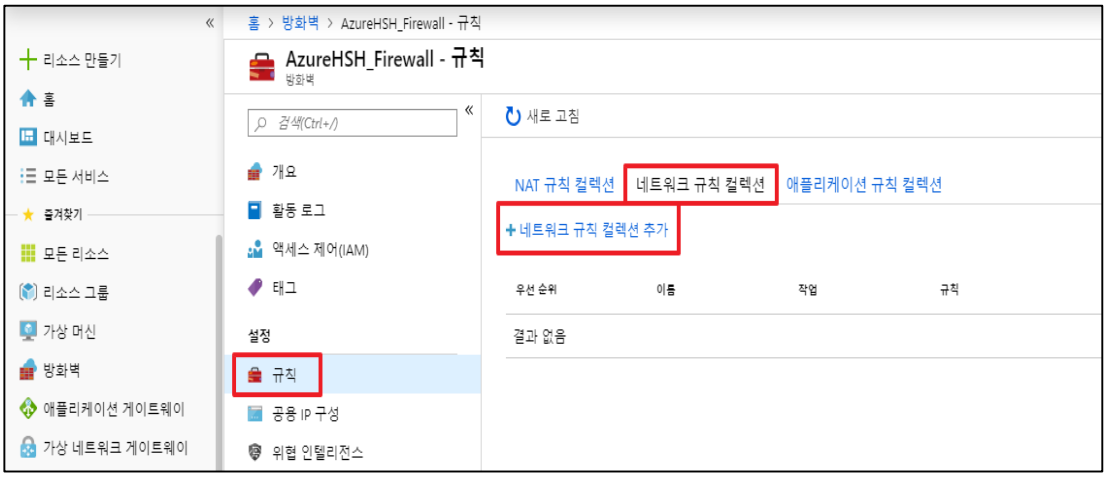
4) 방화벽 정상 생성유무 확인



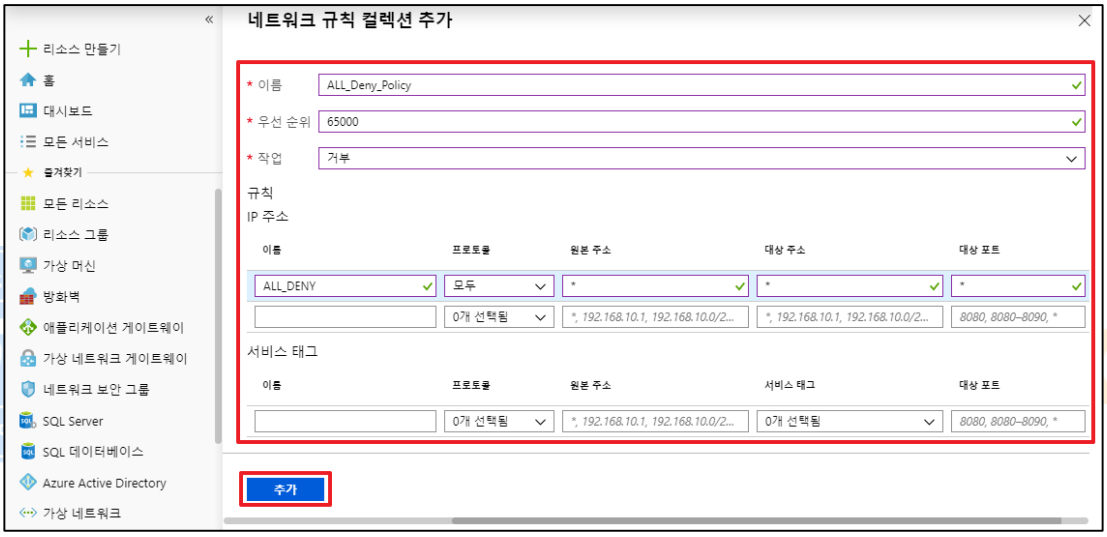
나. 방화벽 네트워크 규칙 생성 방법

1) 방화벽 메뉴 내 네트워크 규칙을 추가할 방화벽 선택

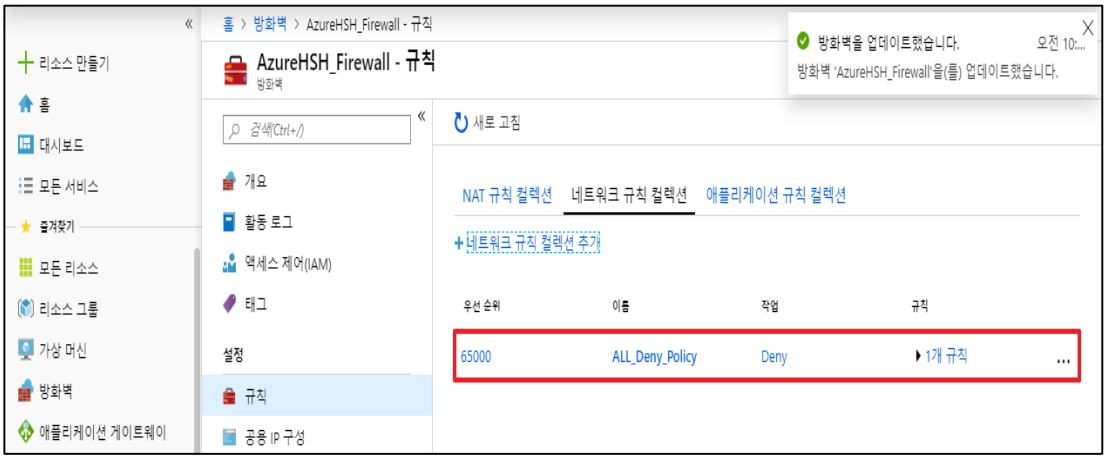
2) 규칙 메뉴 내 네트워크 규칙 컬렉션 추가 버튼 선택



3) 추가할 규칙 설정 및 추가

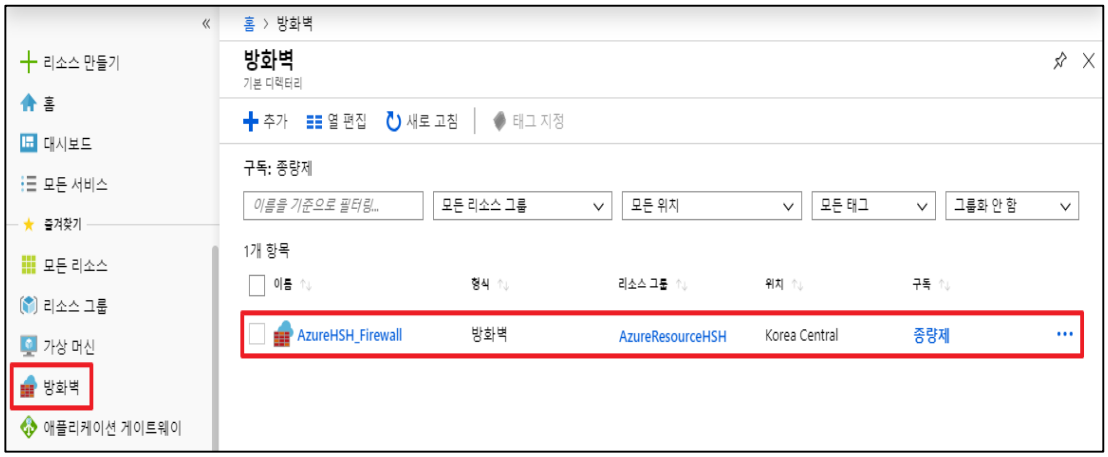


4) 네트워크 규칙 정상 생성유무 확인

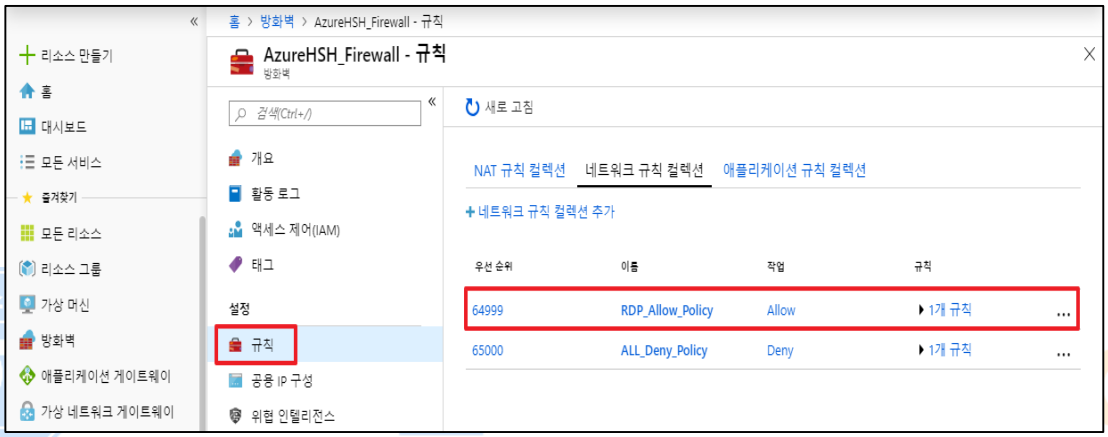


다. 방화벽 네트워크 규칙 삭제 방법

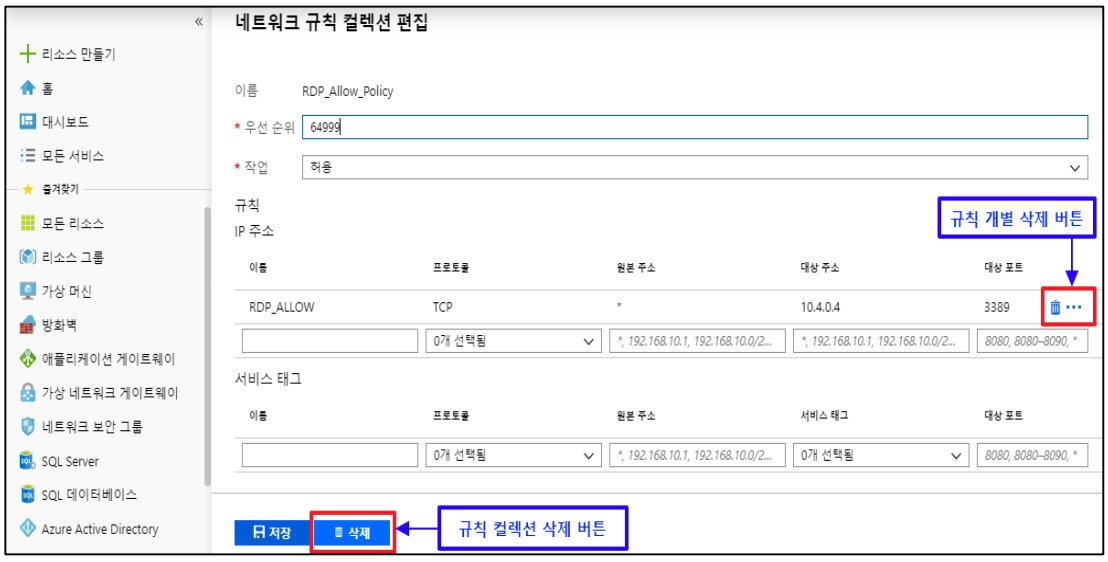
1) 방화벽 메뉴 내 네트워크 규칙을 삭제할 방화벽 선택



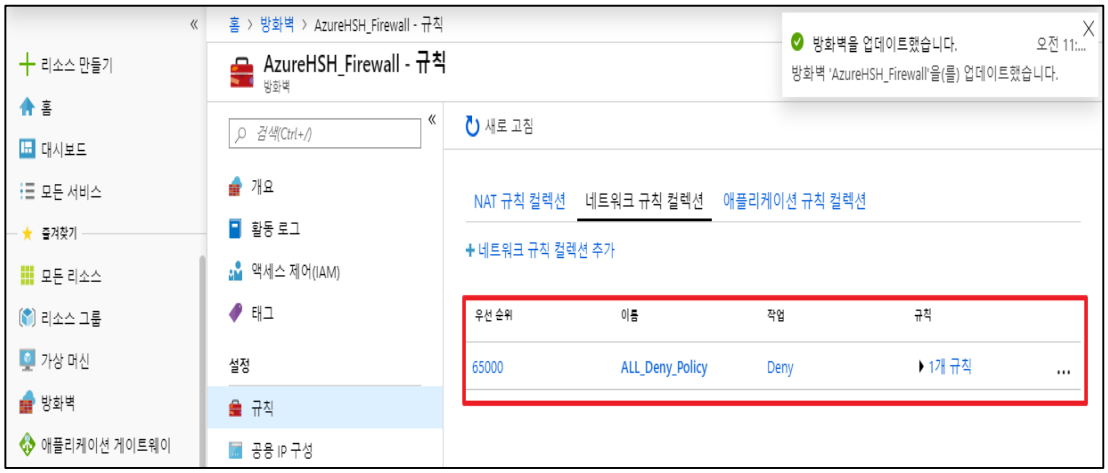
2) 규칙 메뉴 내 네트워크 규칙을 삭제할 규칙 컬렉션 선택



3) 규칙 개별 및 컬렉션 전체 삭제 버튼 선택

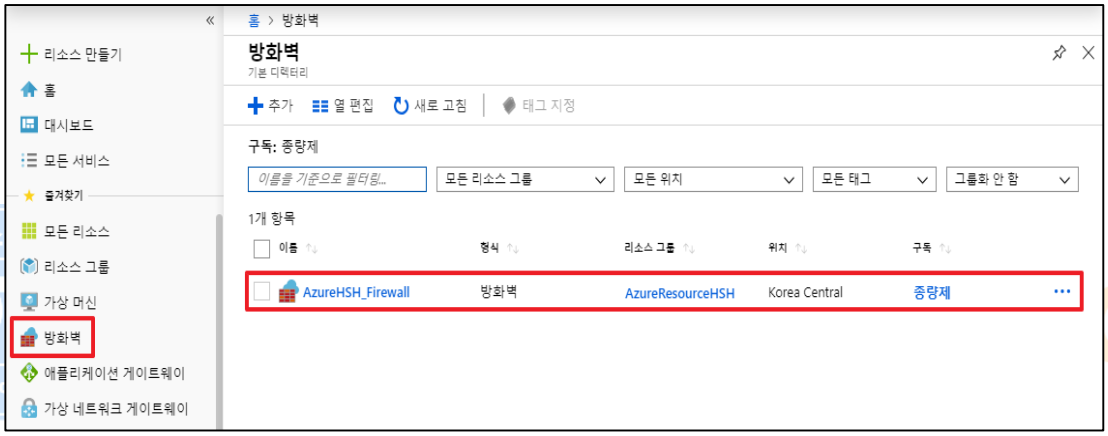


4) 네트워크 규칙 정상 삭제유무 확인



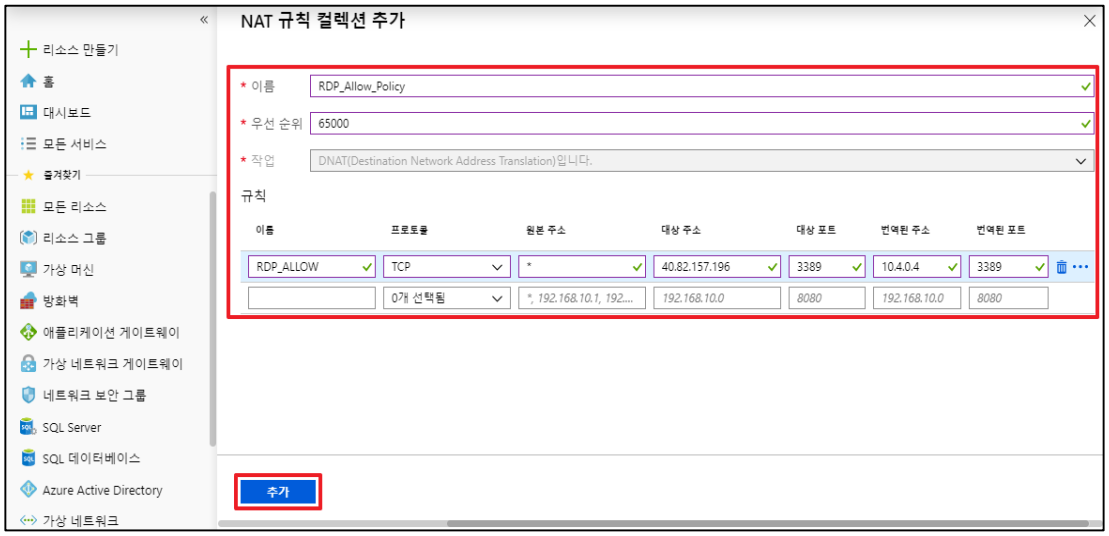
라. 방화벽 NAT 규칙 생성 방법

1) 방화벽 메뉴 내 NAT 규칙을 추가할 방화벽 선택

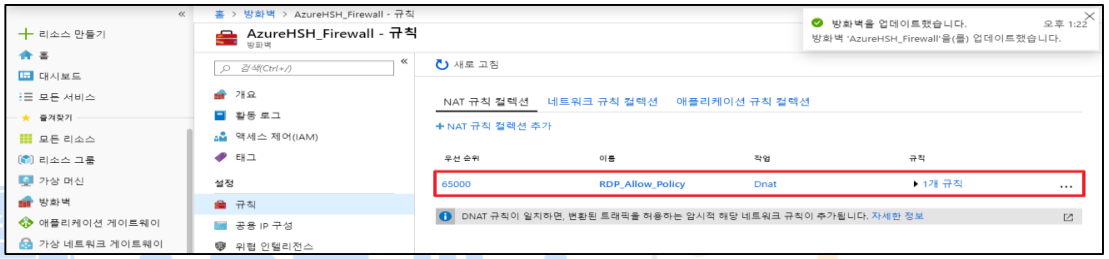


2) 규칙 메뉴 내 NAT 규칙 컬렉션 추가 버튼 선택

3) 추가할 규칙 설정 및 추가

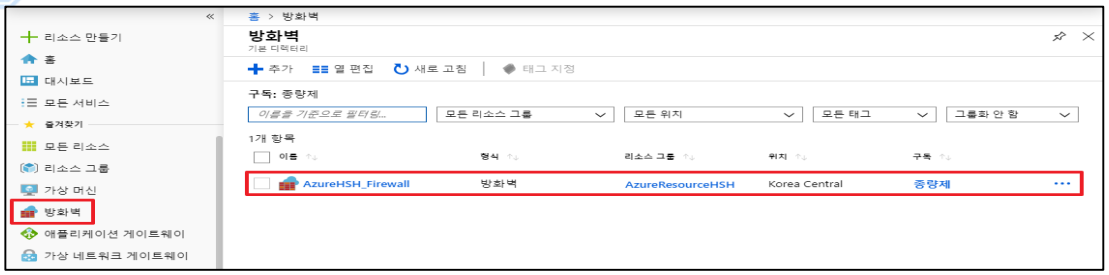


4) NAT 규칙 정상 생성유무 확인

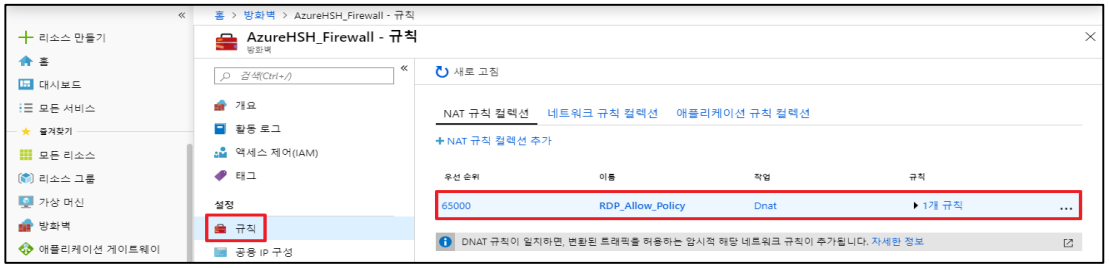


마. 방화벽 NAT 규칙 삭제 방법

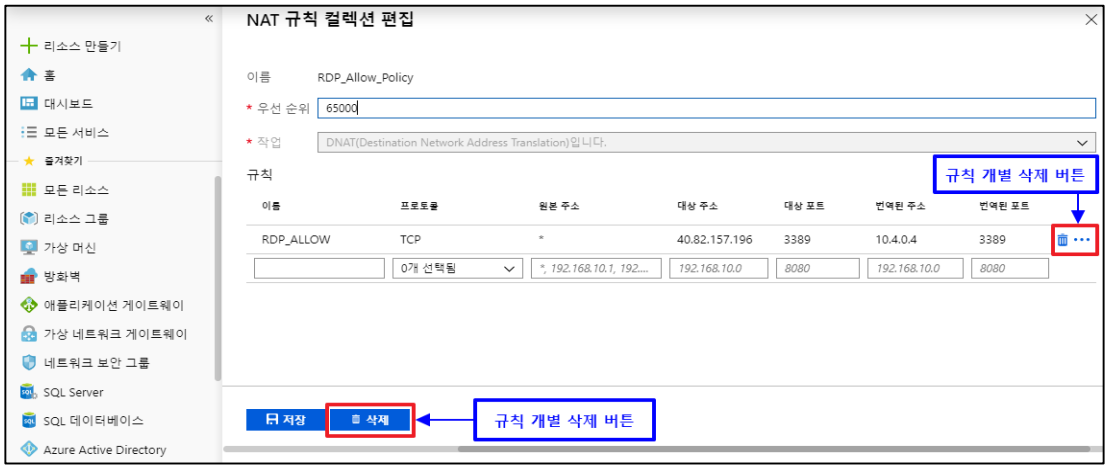
1) 방화벽 메뉴 내 NAT 규칙을 삭제할 방화벽 선택



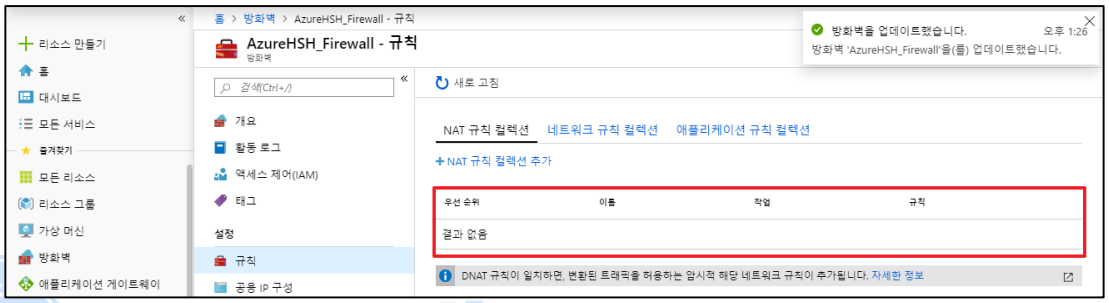
2) 규칙 메뉴 내 NAT 규칙을 삭제할 규칙 컬렉션 선택



3) 규칙 개별 및 컬렉션 전체 삭제 버튼 선택

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


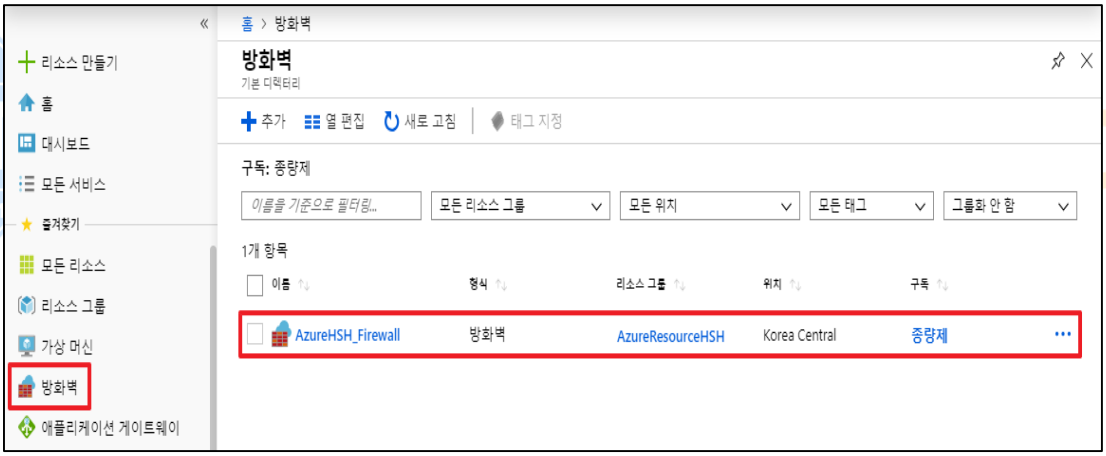
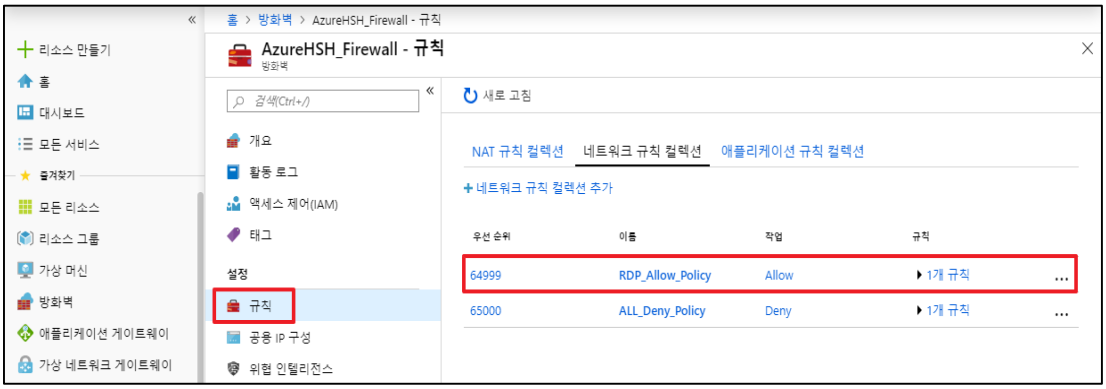
4) NAT 규칙 정상 삭제유무 확인

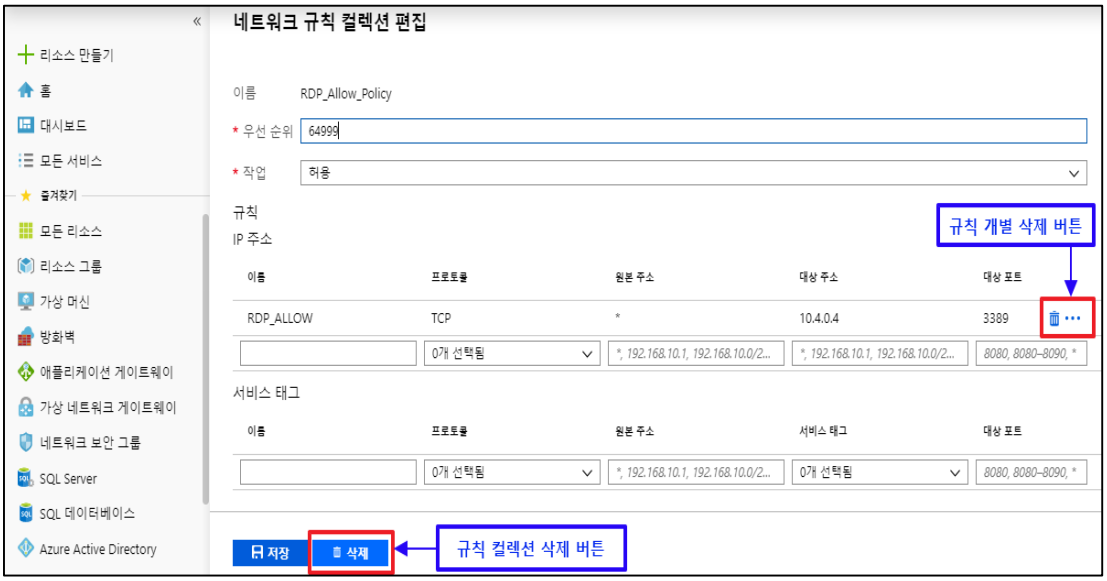


</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 인/아웃바운드 규칙 내 모든 서비스를 Any(IP, Port 등)로 허용하는 정책이 존재하고 있지 않을 경우

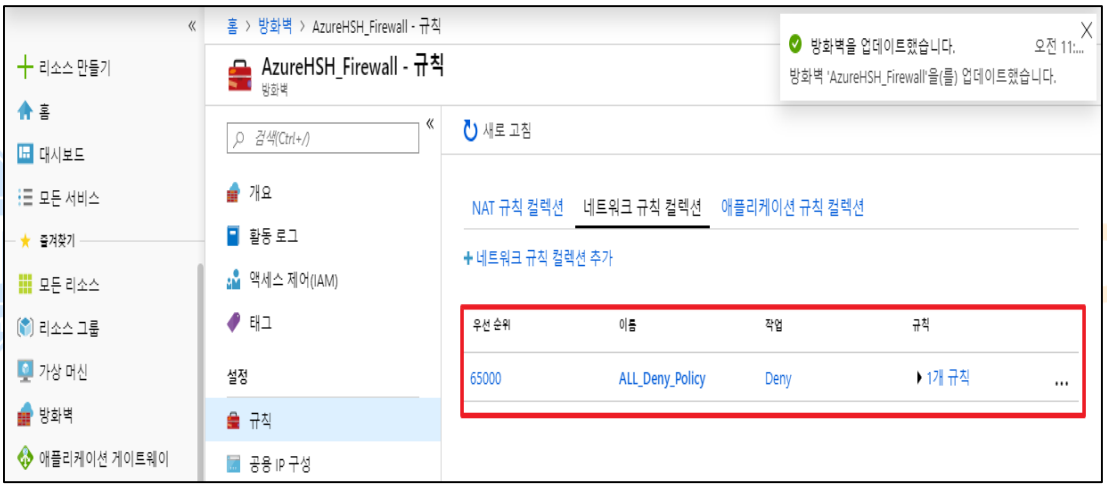
취약기준
: 인/아웃바운드 규칙 내 모든 서비스를 Any(IP, Port 등)로 허용하는 정책이 존재하고 있을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

4.8 방화벽 인/아웃바운드 불필요 정책 관리

분류	가상 리소스 관리	중요도	중
항목명	방화벽 인/아웃바운드 불필요 정책 관리		
항목 설명	Azure Firewall은 Azure Virtual Network 리소스를 보호하는 관리되는 클라우드 기반 네트워크 보안 서비스입니다. 고가용성 및 무제한 클라우드 확장성이 내장되어 있는 서비스 형태의 완전한 상태 저장 방화벽입니다. 인/아웃바운드 트래픽 내 불필요한 정책이 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 정책이 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) 규칙 개별 및 컬렉션 전체 삭제 버튼 선택		

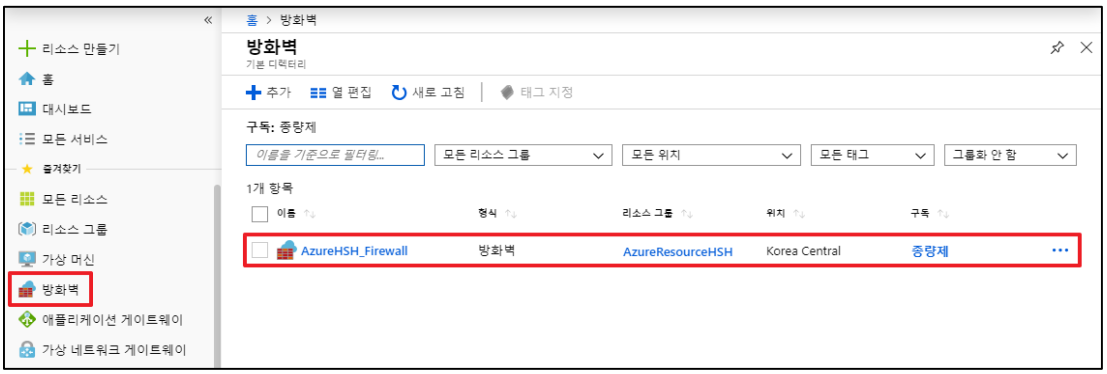


4) 네트워크 규칙 정상 삭제유무 확인

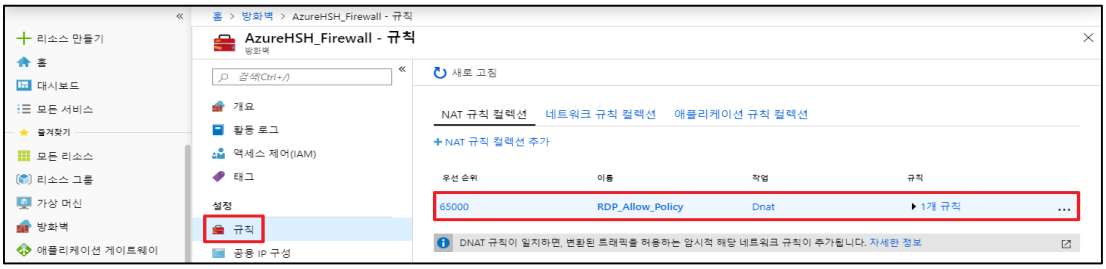


나. 방화벽 내 불필요한 NAT 규칙 삭제 방법

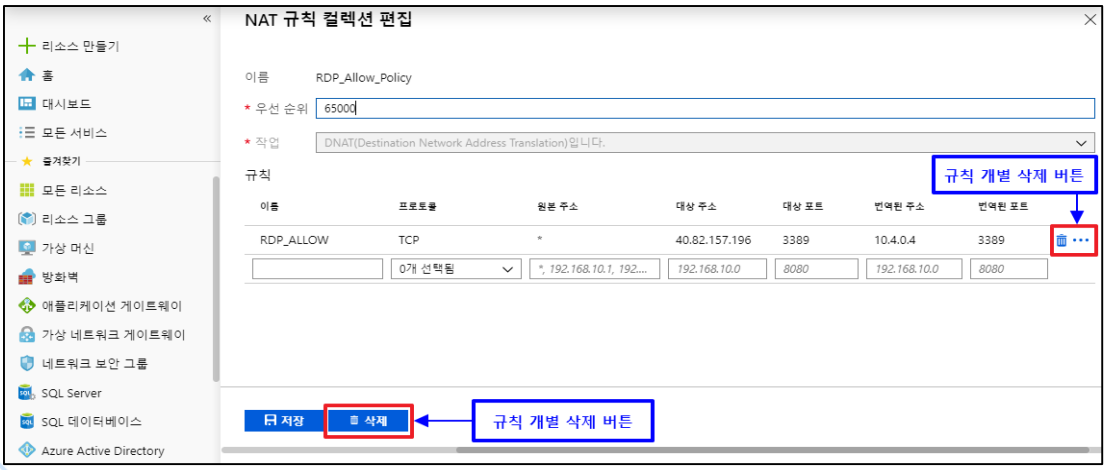
1) 방화벽 메뉴 내 NAT 규칙을 삭제할 방화벽 선택



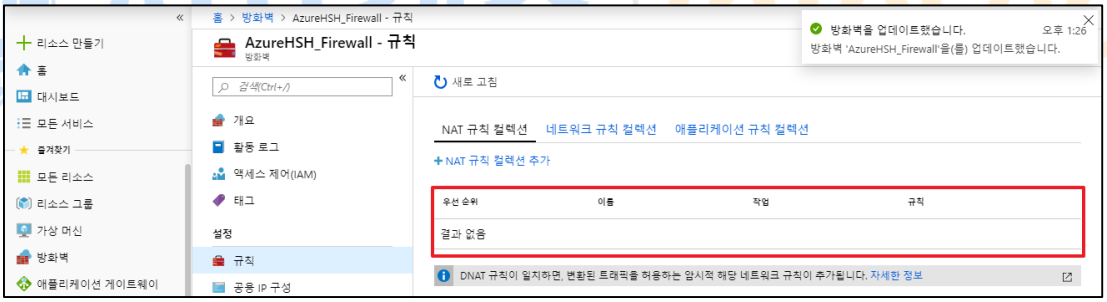
2) 규칙 메뉴 내 NAT 규칙을 삭제할 규칙 컬렉션 선택



3) 규칙 개별 및 컬렉션 전체 삭제 버튼 선택

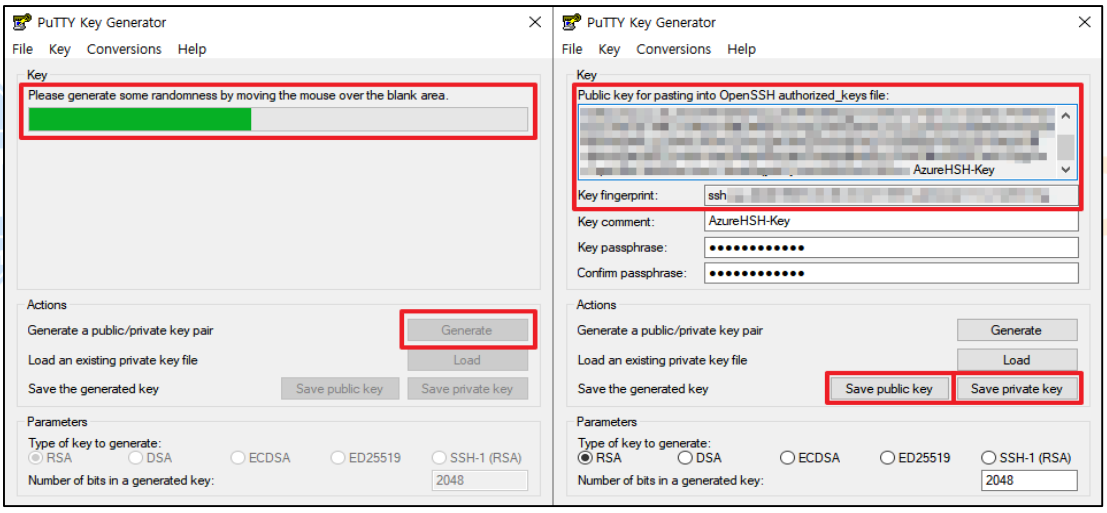
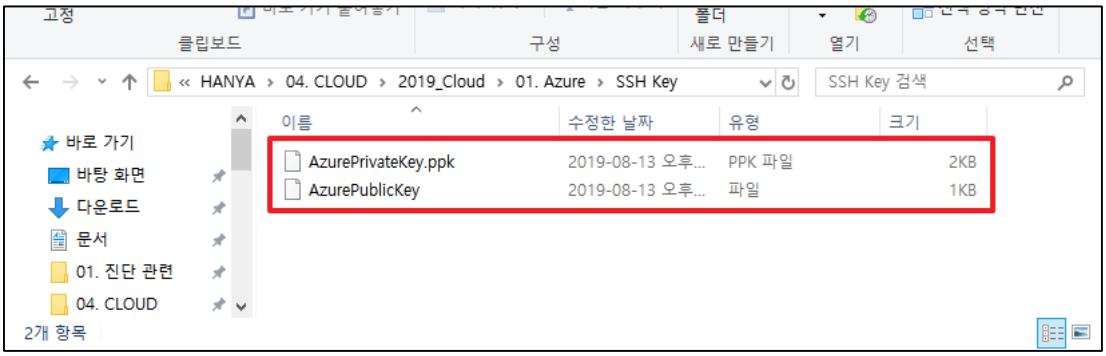


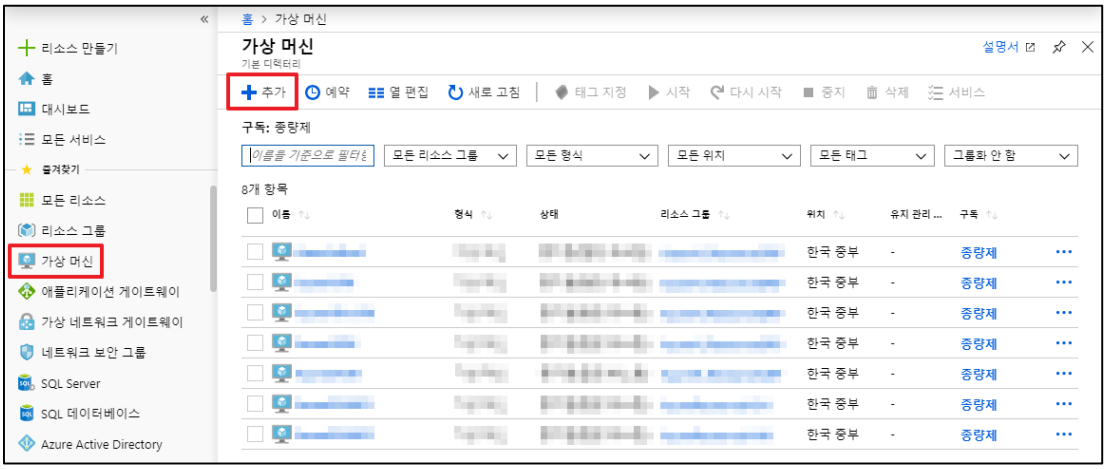
4) NAT 규칙 정상 삭제유무 확인



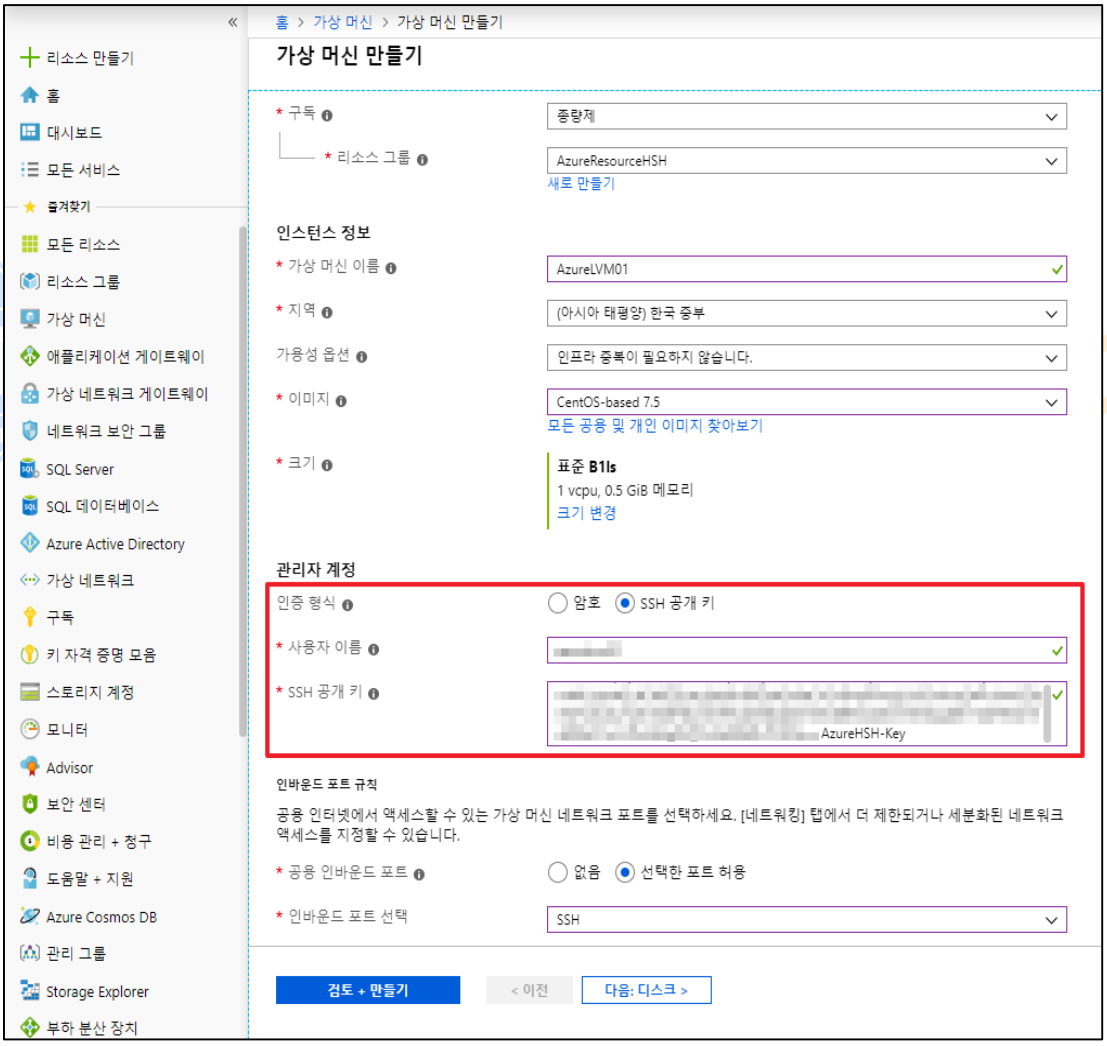
진단 기준	**양호기준** : 인/아웃바운드 규칙 내 서비스 목적을 알 수 없는 정책이 존재하고 있지 않을 경우 **취약기준** : 인/아웃바운드 규칙 내 서비스 목적을 알 수 없는 정책이 존재하고 있을 경우
비고	

4.9 가상 Compute 안전한 SSH 연결

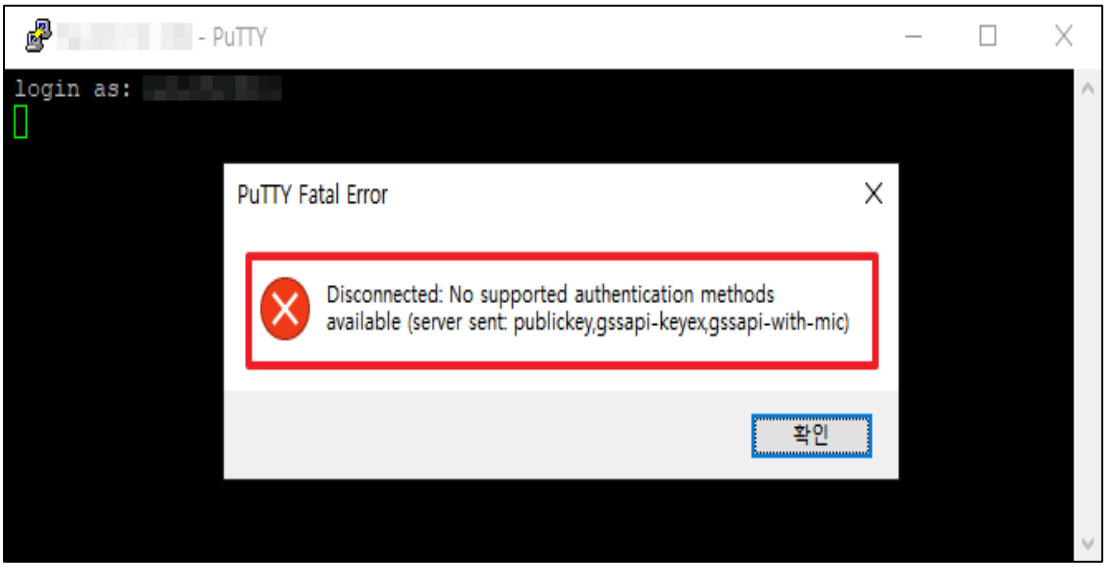
분류	가상 리소스 관리	중요도	중
항목명	가상 Compute 안전한 SSH 연결		
항목 설명	SSH는 암호화된 연결을 통해 Azure에서 호스팅하는 Linux VM에 안전하게 로그인할 수 있도록 하는 기본 연결 프로토콜입니다. SSH 자체에서 암호화된 연결을 제공하지만 SSH 연결과 함께 암호를 하더라도 VM은 여전히 무차별 암호 대입 공격이나 암호 추측에 취약하기 때문에, SSH를 사용하여 VM에 연결하는 데 있어 더 안전하고 선호하는 방법은 SSH Key라고도 하는 공개-개인 키 쌍을 사용하는 것입니다. SSH(보안 셸) 키 쌍을 사용하면 인증을 위해 기본적으로 SSH Key를 사용하는 Linux 가상 머신을 Azure에서 만들 수 있으므로 로그인할 때 암호가 필요하지 않습니다. Azure Portal, Azure CLI, Resource Manager 템플릿 또는 기타 도구를 사용하여 만든 VM은 SSH 연결을 위해 SSH Key 인증을 설정하는 배포의 일부로 SSH Public Key를 포함할 수 있습니다.		
설정 방법	**가. SSH Key(Public, Private Key) 생성 방법** 1) PuTTYGen을 통한 SSH Key 생성(Linux 계열은 ssh-keygen, Windows계열은 PuTTYGen)  2) 생성된 SSH Key 파일을 쉽게 유추하거나 접근할 수 없는 공간에 보관  **나. 가상머신 생성 시 초기 SSH Key 설정 방법** 1) 가상머신 메뉴 내 가상머신 추가 버튼 선택		



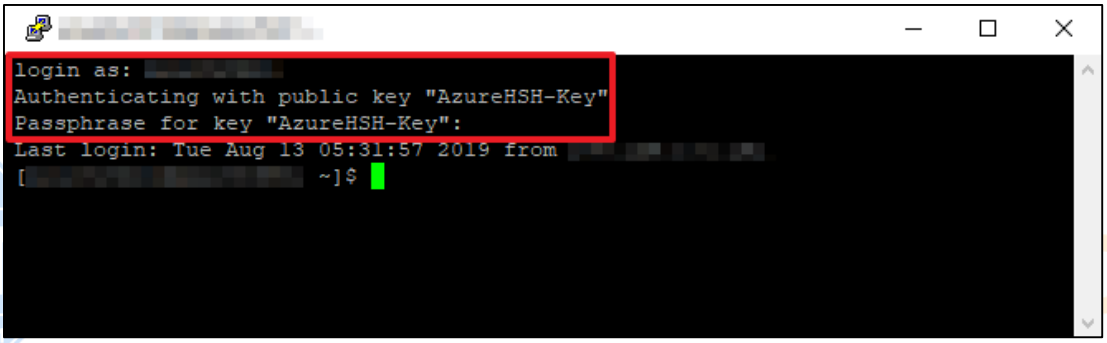
2) 가상머신 관련 값 설정 시 인증형식을 SSH 공개 키로 선택 후 공개 키 등록 및 만들기



3) 가상머신에 SSH Key 등록 후 아이디로만 접근시도 했을 경우 (비정상)

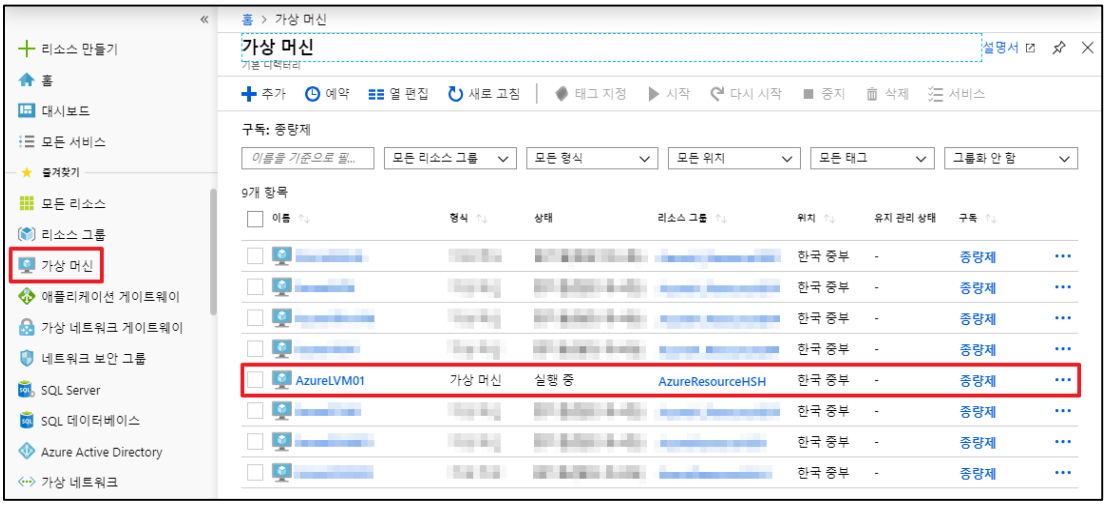


4) 가상머신에 SSH Key 등록 후 아이디, SSH Key로 접근시도 했을 경우 (정상)

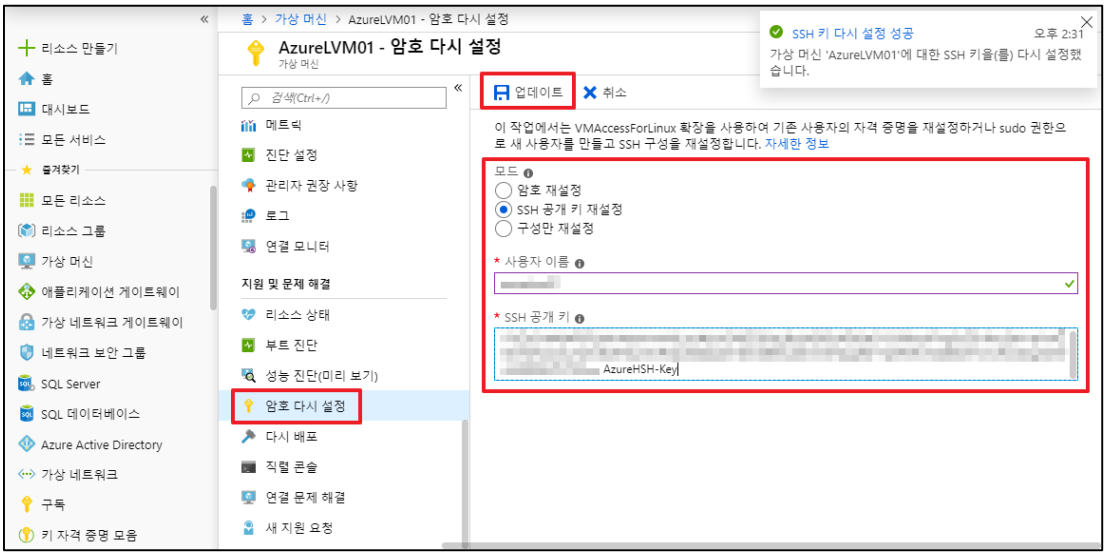


다. SSH Key 변경 설정 방법

1) 가상머신 메뉴 내 SSH Key를 변경할 가상머신 선택

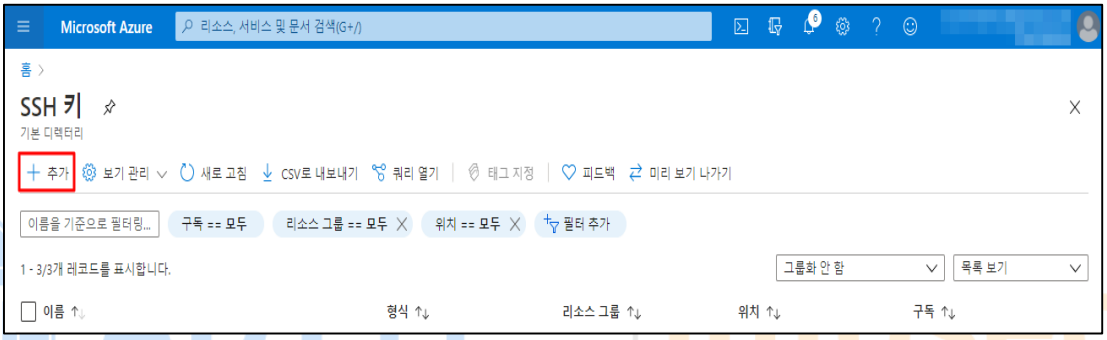
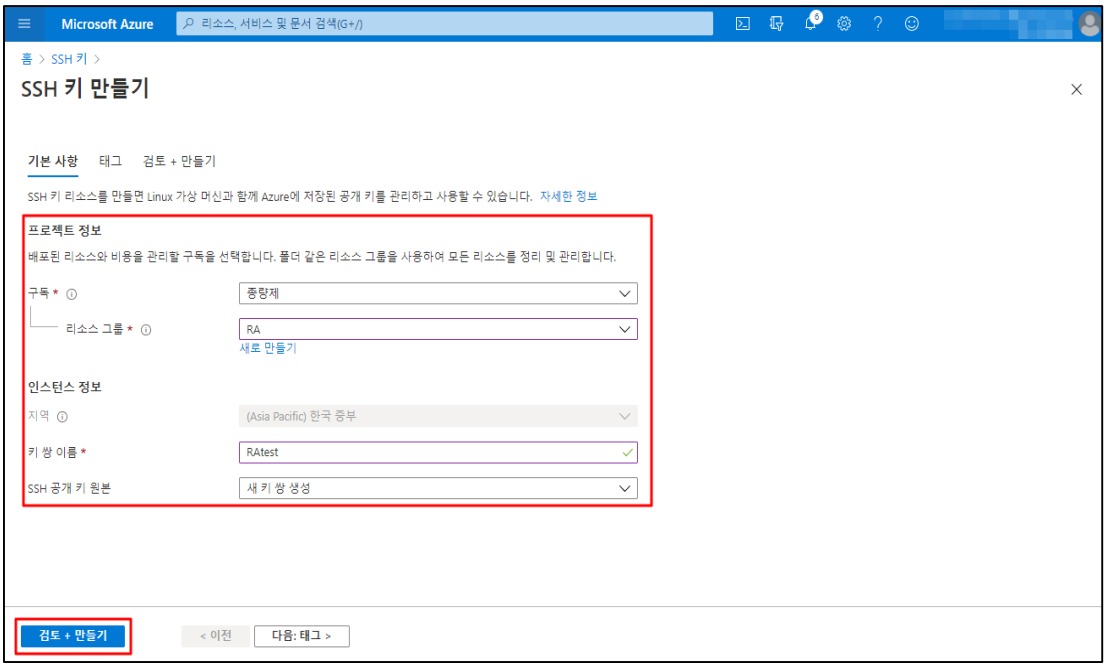


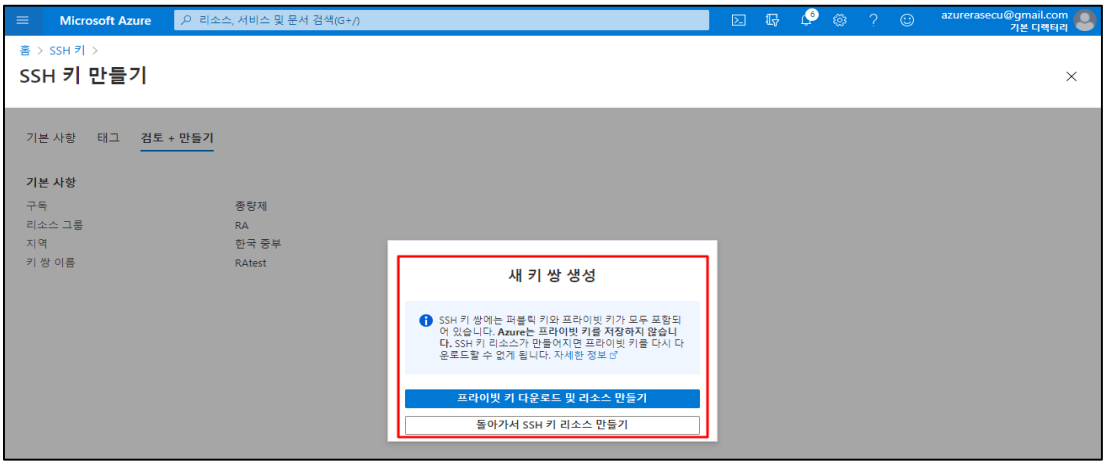
2) 암호 다시 설정 메뉴 내 SSH Key 재등록 및 업데이트

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: SSH Key 를 통해 가상 Compute 에 접근하도록 설정되어 있을 경우

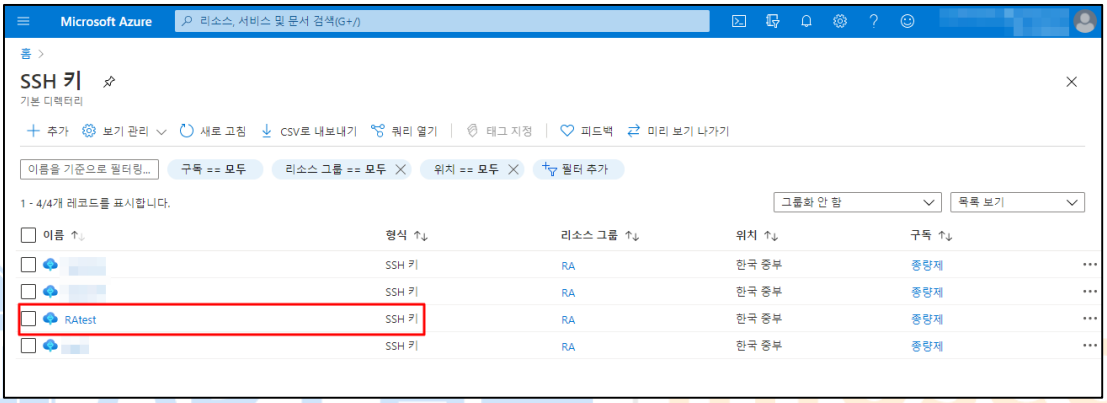
취약기준
: SSH Key 를 통해 가상 Compute 에 접근하도록 설정되어 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

4.10 SSH Key 관리

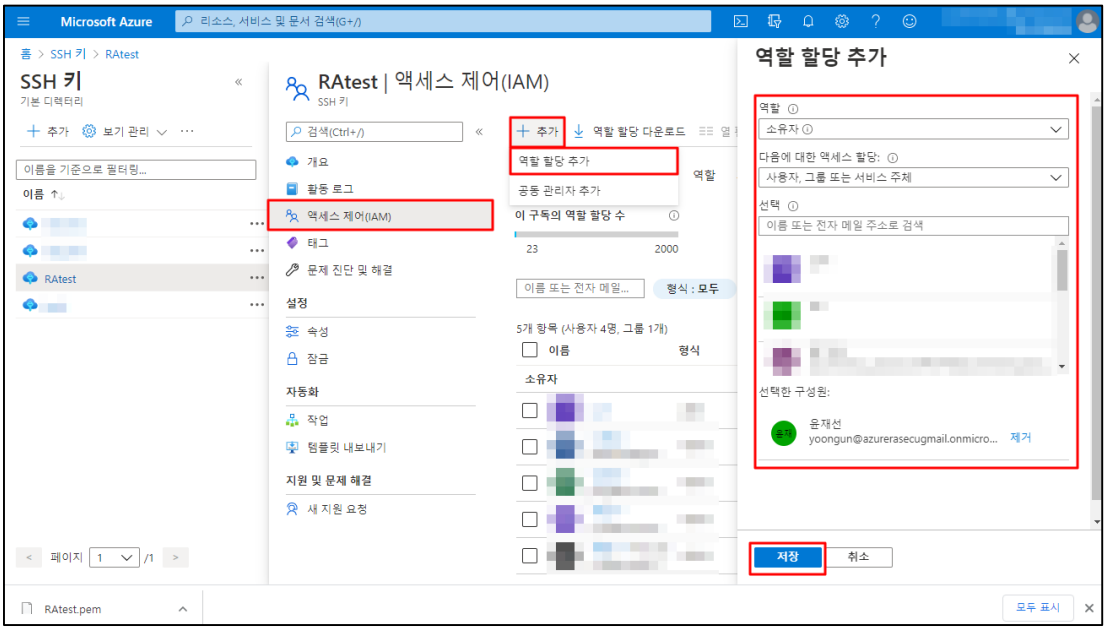
분류	가상 리소스 관리	중요도	하
항목명	SSH Key 관리		
항목 설명	SSH 키는 기존의 "키 페어(pem)"와 동일한 방식의 공개-개인 키 쌍을 사용하여 SSH를 통해 가상머신으로 접근이 가능합니다. SSH 키는 AZURE 포탈을 통해 생성 할 수 있으며 해당 키는 가상 머신에 적용하여 사용할 수 있습니다. SSH 키를 통해 가상 머신으로 직접 접근이 가능한 보안 키로 불필요한 사용자 및 비인가된 사용자가 액세스 제어(IAM) 사용자/그룹 역할이 적용될 경우 가상머신 리소스에 접근이 가능해지는 문제가 발생할 수 있습니다.		
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		



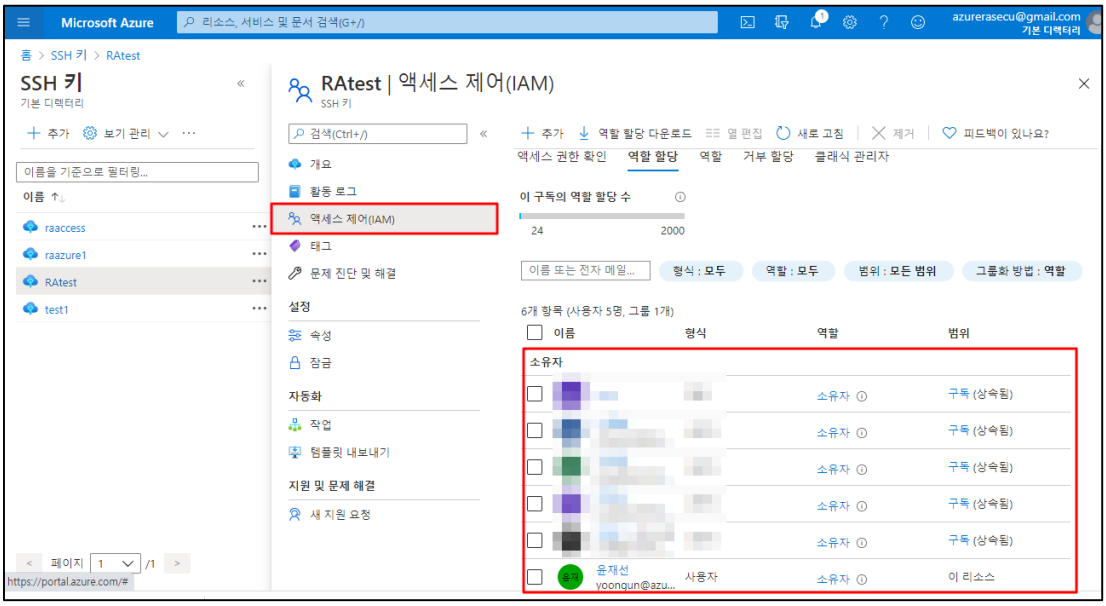
4) 생성된 SSH 키 확인



5) SSH 키의 액세스 제어(IAM) 역할 할당 추가



6) SSH 키의 액세스 제어(IAM) 리스트 확인

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>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</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

4.11 스토리지 계정 보안 설정

분류	가상 리소스 관리	중요도	상
항목명	스토리지 계정 보안 설정		

항목 설명

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 고가용성을 제공하며 안전하고 대규모로 확장 가능합니다.

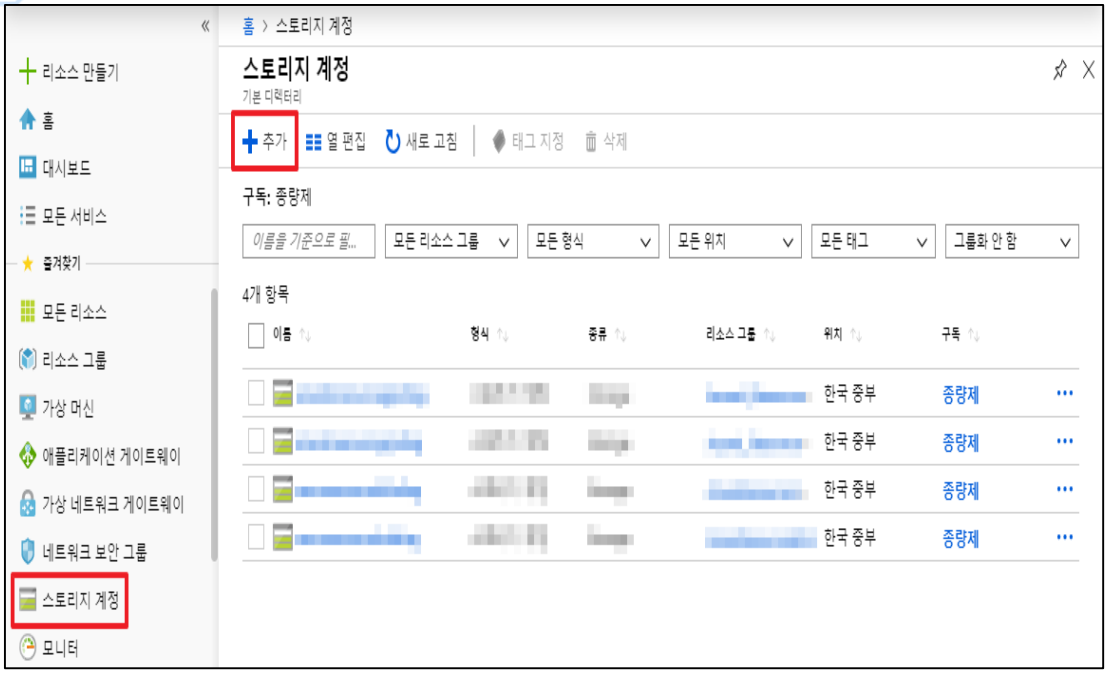
※ 스토리지 계정 생성 시 보안옵션

옵션	내용	기준값
보안전송	HTTP 프로토콜을 사용한 요청에 대한 요청 거부 유무	사용
가상네트워크 액세스 허용	액세스 허용하는 가상네트워크를 전체 또는 일부 네트워크 선택	선택된 네트워크
데이터 보호	Blob 일시삭제를 통해 응용 프로그램 또는 다른 스토리지 계정 사용자에 의해 잘못 수정되거나 삭제될 때 데이터를 보다 쉽게 복구	-
계층구조 네임스페이스	빅데이터 워크로드 분석을 가속화하고 파일단위 ACL을 활성화	-

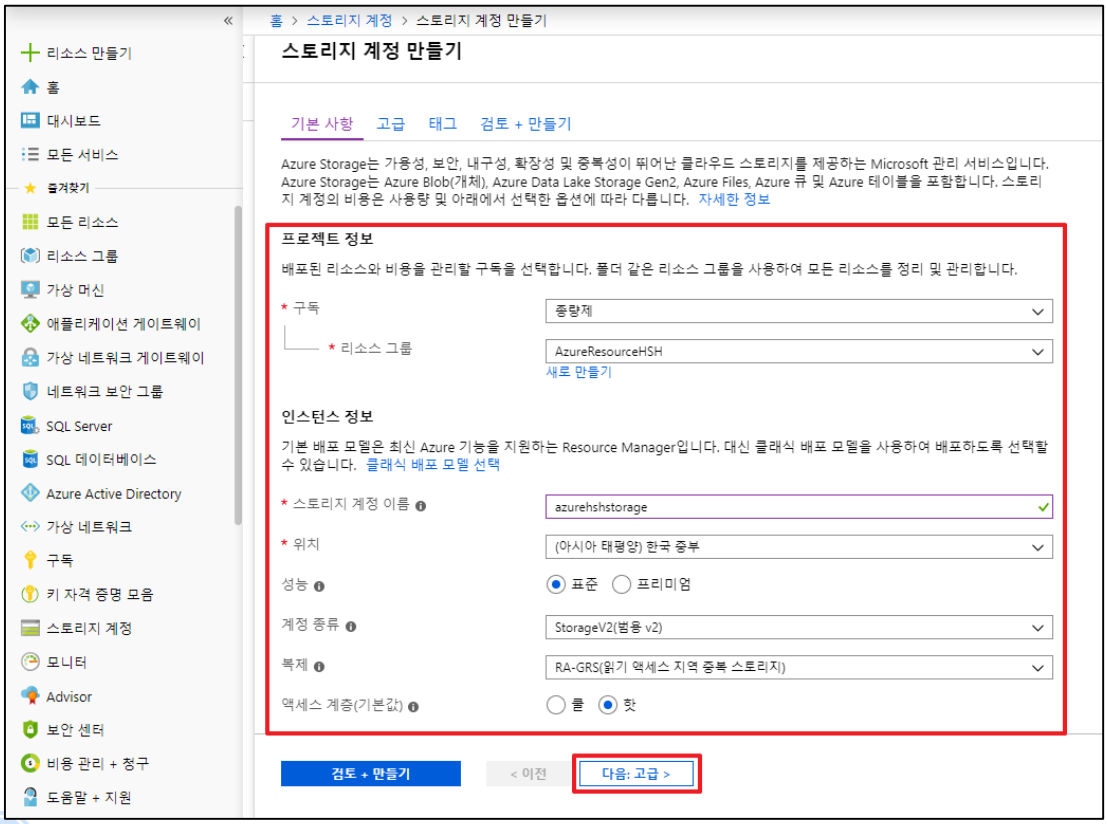
설정 방법

가. 스토리지 계정 생성 방법

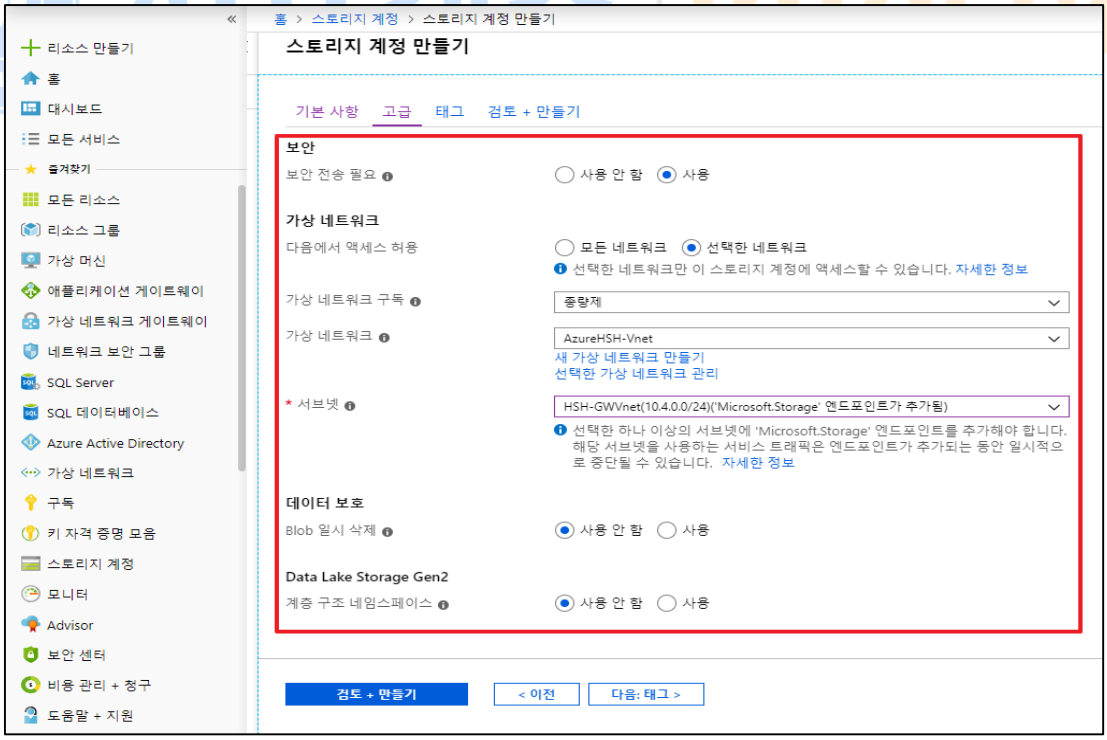
1) 스토리지 계정 메뉴 내 스토리지 계정 추가 버튼 선택



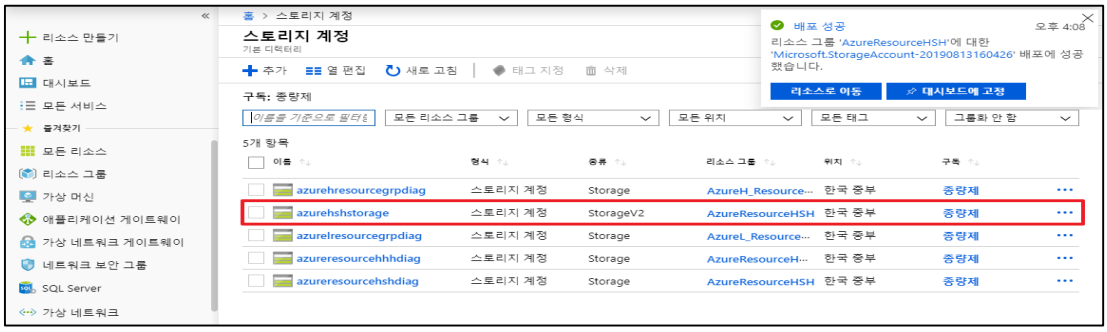
2) 스토리지 계정 관련 기본 사항 값 설정



3) 스토리지 계정 관련 고급(보안전송 및 가상 네트워크 허용) 값 설정 및 만들기

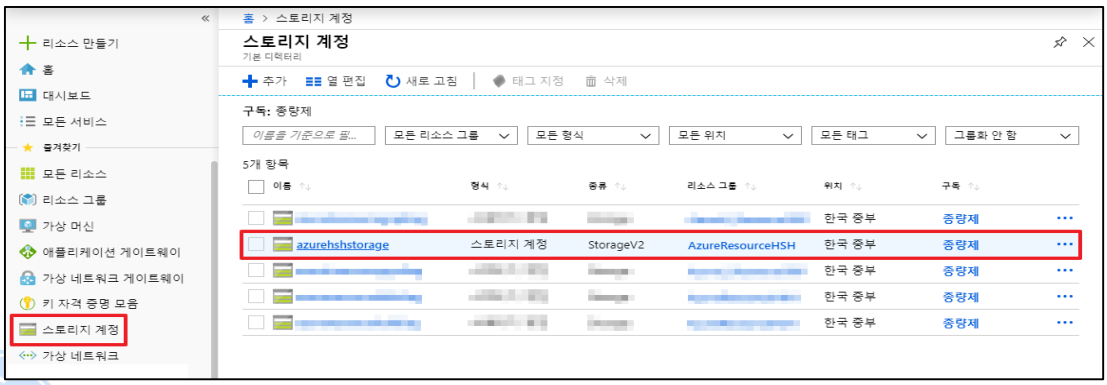


4) 스토리지 계정 목록 내 정상 생성유무 확인

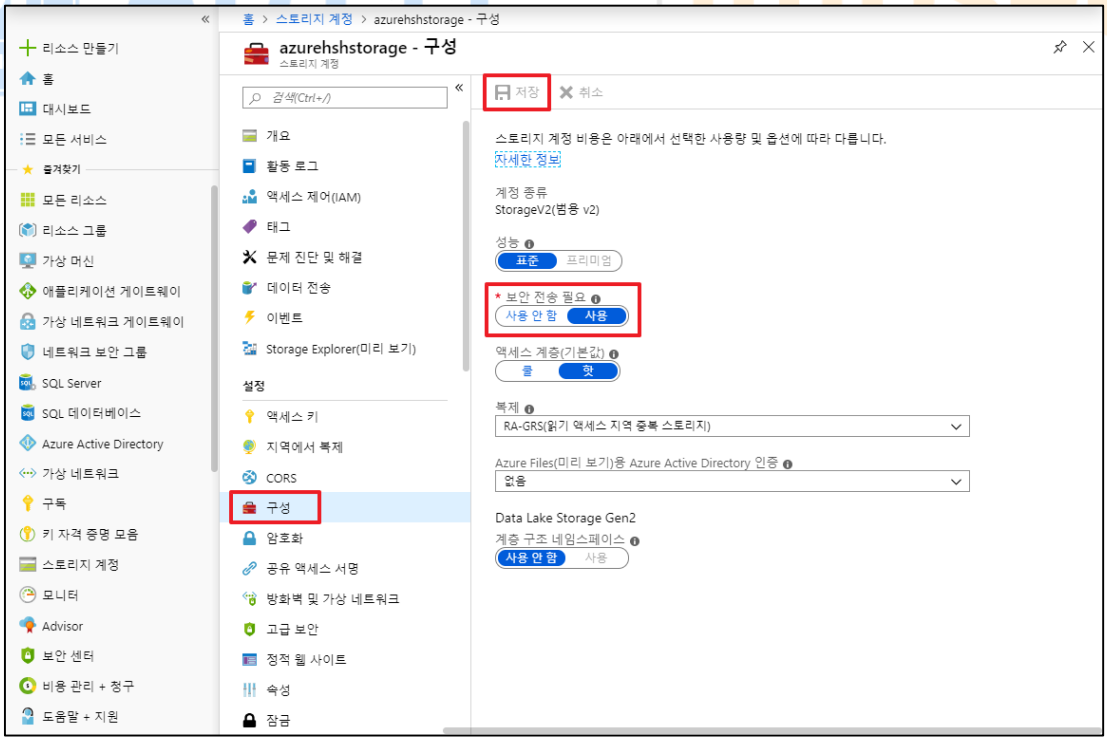


나. 스토리지 계정 보안옵션(보안전송, 가상 네트워크 액세스 허용) 변경 방법

1) 스토리지 계정 메뉴 내 보안옵션을 변경할 스토리지 계정 선택

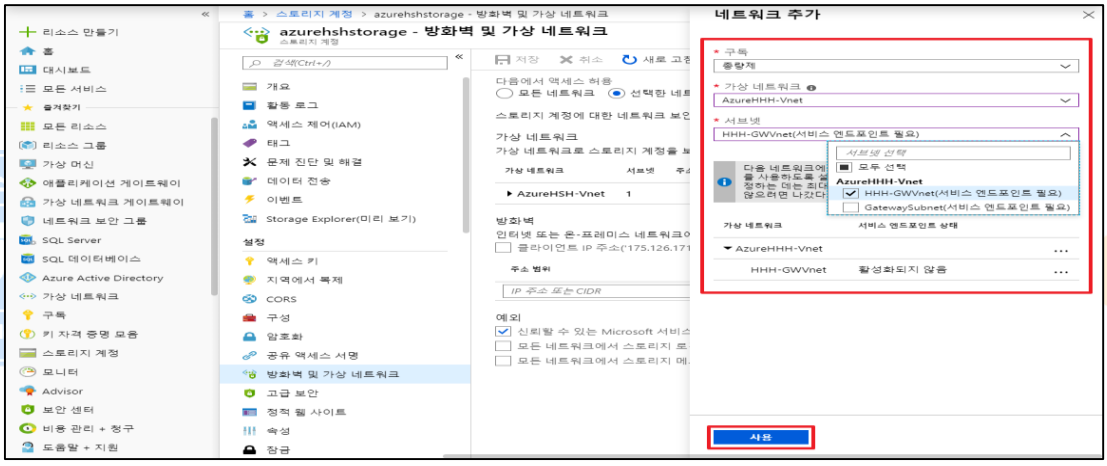


2) 구성 메뉴 내 보안 전송 필요 옵션 사용으로 설정

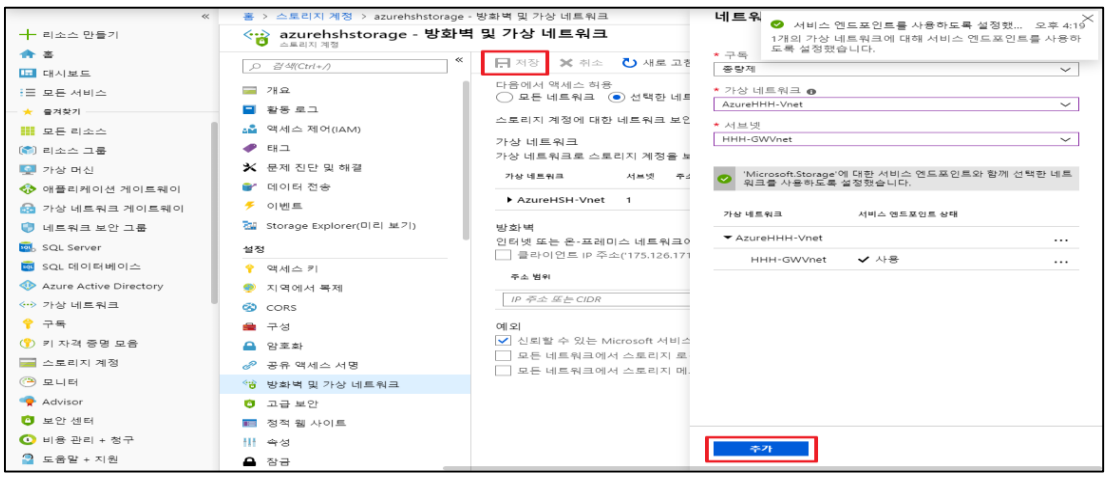


3) 방화벽 및 가상 네트워크 메뉴 내 네트워크 허용 및 허용할 가상 네트워크 추가 버튼 선택

4) 허용할 가상 네트워크 및 서브넷 선택 및 사용 버튼 선택



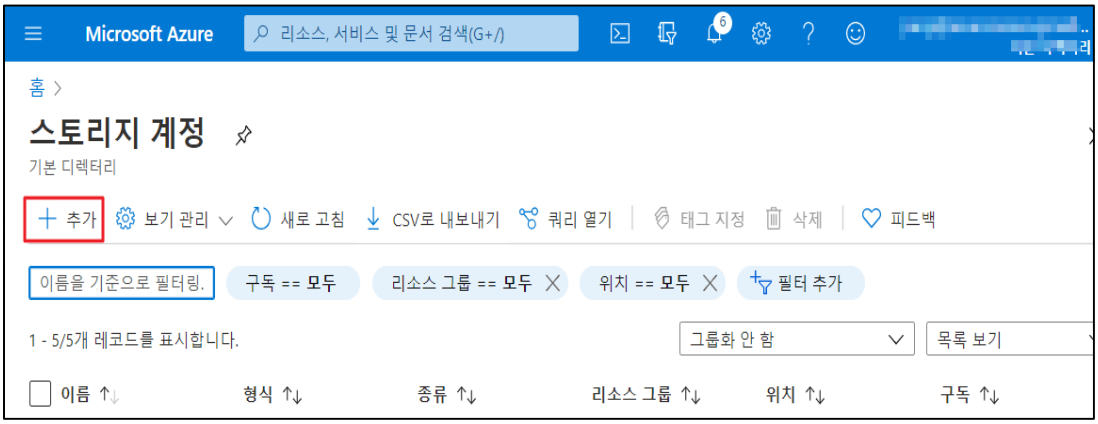
5) 네트워크 허용 정상 추가여부 확인 및 저장



진단 기준	양호기준 : 보안옵션(보안전송, 가상 네트워크 액세스 허용)을 사용하여 스토리지 계정을 생성했을

	경우 **취약기준** : 보안옵션(보안전송, 가상 네트워크 액세스 허용)을 사용하여 스토리지 계정을 생성하지 않을 경우
비고	

4.12 스토리지 계정 권한 관리

분류	가상 리소스 관리	중요도	상
항목명	스토리지 계정 권한 관리		
항목 설명	Active Directory 그룹을 통한 Active Directory 사용자에게 권한을 부여해 스토리지 계정 관련 기능/서비스를 이용할 경우 사용 및 설정(접근, 생성, 수정, 삭제)에 대한 직무 기준 및 관리 방안을 수립 해야합니다. 또한, 그룹 별 Active Directory 사용자에 대한 직무 구분 및 역할에 맞는 사용자 권한이 설정되어야 하며 권한 오.남용이 발생하지 않도록 관리되어야 합니다. 또한 직무를 수행하는 임직원에 대한 그 목록을 최신으로 관리해야 합니다. 아래는 주요 직무의 기준 및 직무분리 예시를 설명합니다. **1) 주요 직무의 기준 예시** - 중요정보 (개인정보, 인사정보, 영업비밀, 산업기밀, 재무정보 등) 취급 - 중요 정보 시스템 (서버, DB, 응용 프로그램 등) 및 개인정보처리 시스템 운영 관리 - 정보보호 및 개인정보보호 관리 업무 수행 - 보안 시스템 운영 등 **2) 직무 분리 기준** - 개발과 운영 직무 분리 - 정보보호담당자, 개인정보취급자와 정보보호 및 개인정보 모니터링 직무 분리 - 정보시스템 및 개인정보처리시스템(서버, DB, 네트워크 등)간 운영직무 분리 - 정보보호 및 개인정보보호 관리와 정보보호 및 개인정보보호 감사 업무 분리 - 개인정보보호 관리와 개인정보처리시스템 운영직무 분리 - 개인정보보호 관리와 개인정보처리시스템 개발직무 분리 등 - 외부 위탁업체 직원에게 사용자 계정 등록, 삭제(비활성화) 및 접근권한 등록, 변경, 삭제 설정 권한 부여 금지(단, 불가피한 경우 보완통제 적용)		
설정 방법	**가. 스토리지 설정** 1) 스토리지 계정 추가  2) 스토리지 계정 만들기 - 기본사항		

3) 스토리지 계정 만들기 - 네트워킹

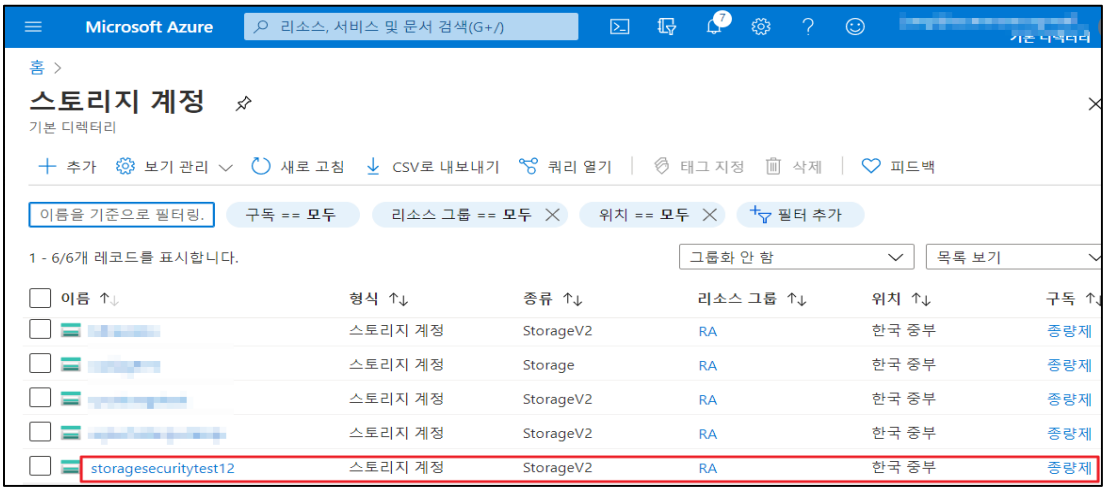
4) 스토리지 계정 만들기 - 데이터 보호

5) 스토리지 계정 만들기 - 고급

6) 스토리지 계정 만들기 - 태그

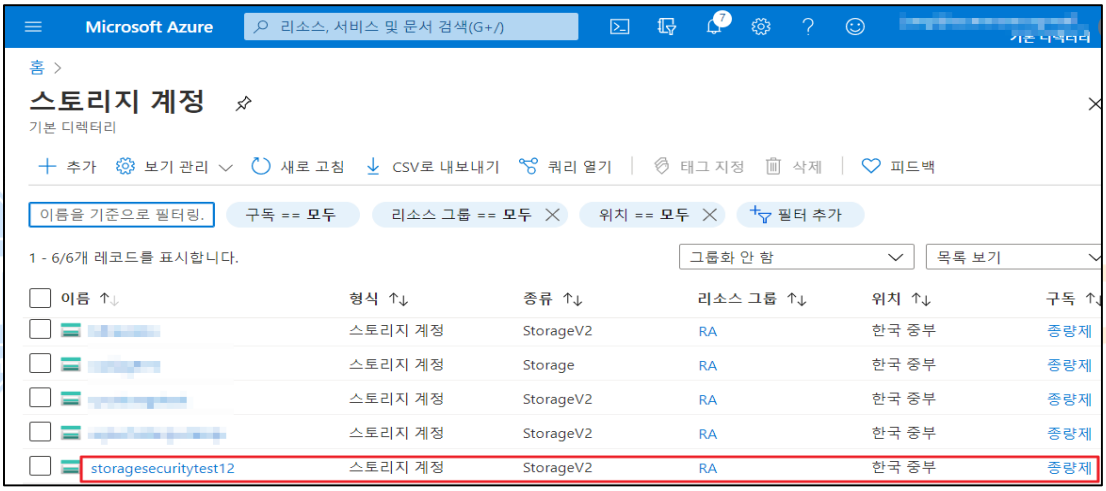
7) 스토리지 계정 만들기 - 검토

8) 스토리지 계정 생성 확인

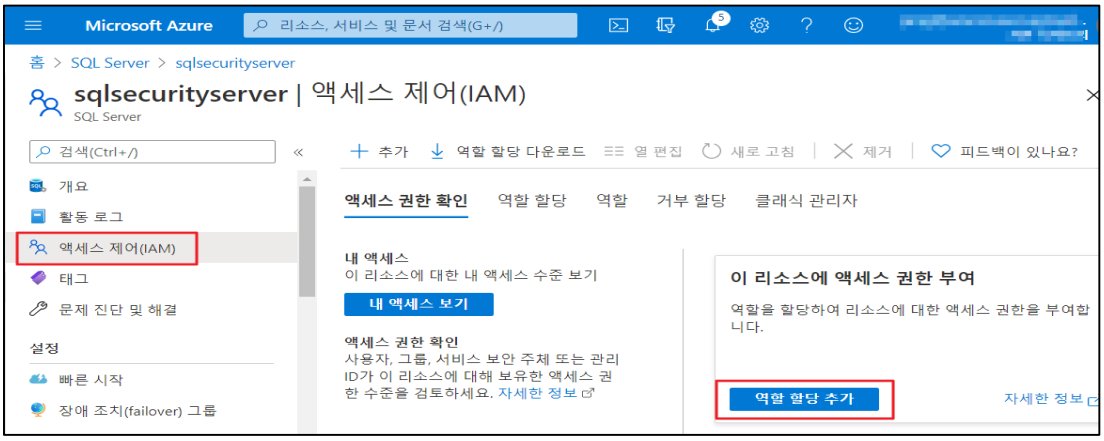


나. 스토리지 역할 설정

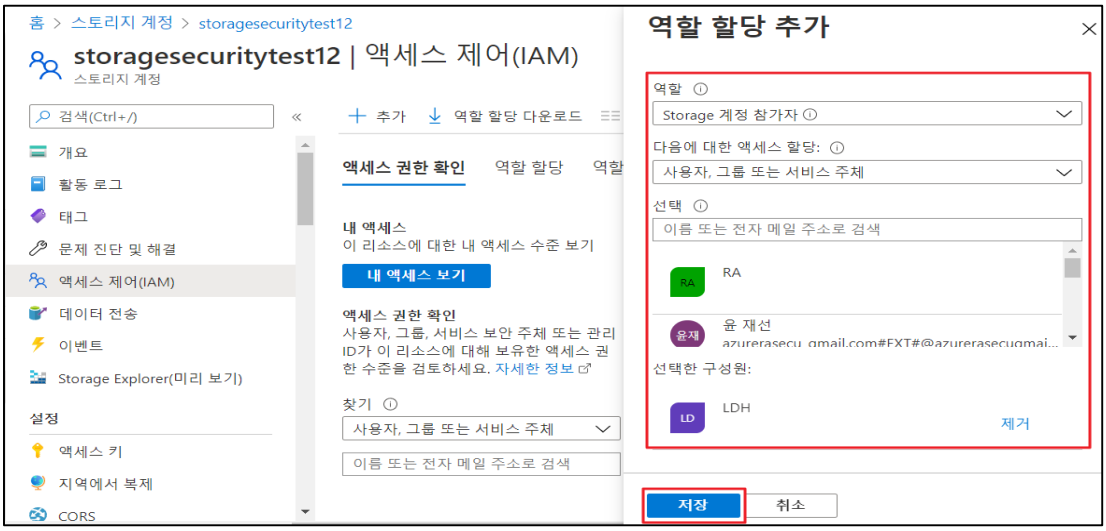
1) 스토리지 역할 추가



2-1) 스토리지 액세스 제어(IAM) 역할 추가



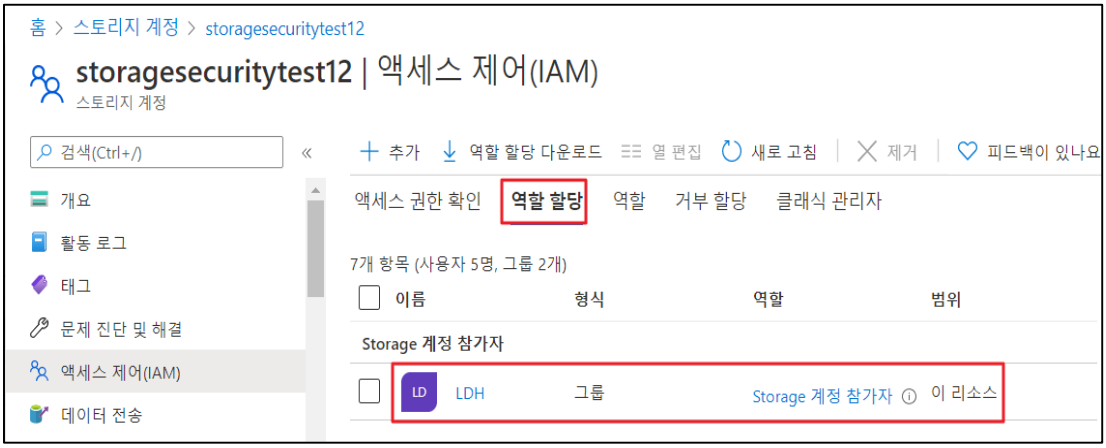
2-2) 스토리지 액세스 제어(IAM) 역할 추가



3) 추가된 액세스 제어(IAM) 확인

다. 스토리지 액세스 제어(IAM) 역할 확인

1) 액세스 제어(IAM) 확인



진단 기준

양호기준

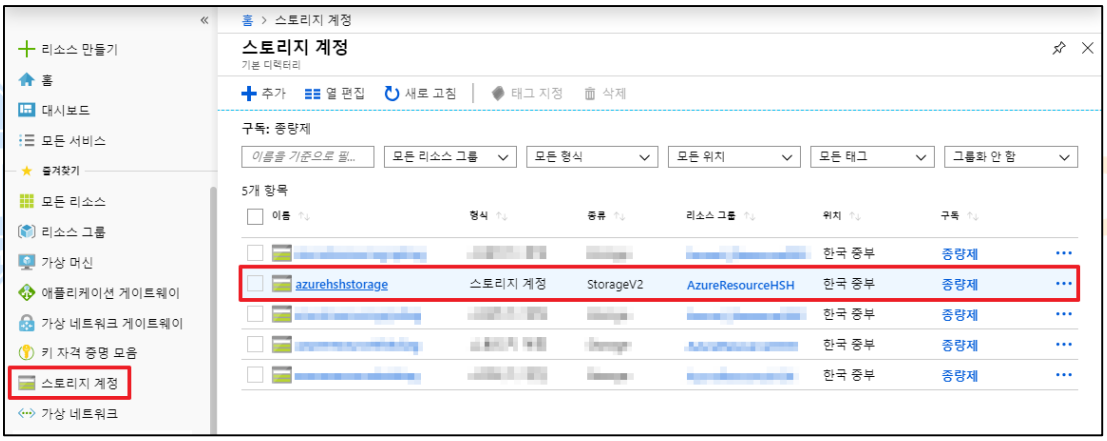
: IAM 의 사용자 및 권한에 맞게 발급된 스토리지 계정을 운영하고 있을 경우

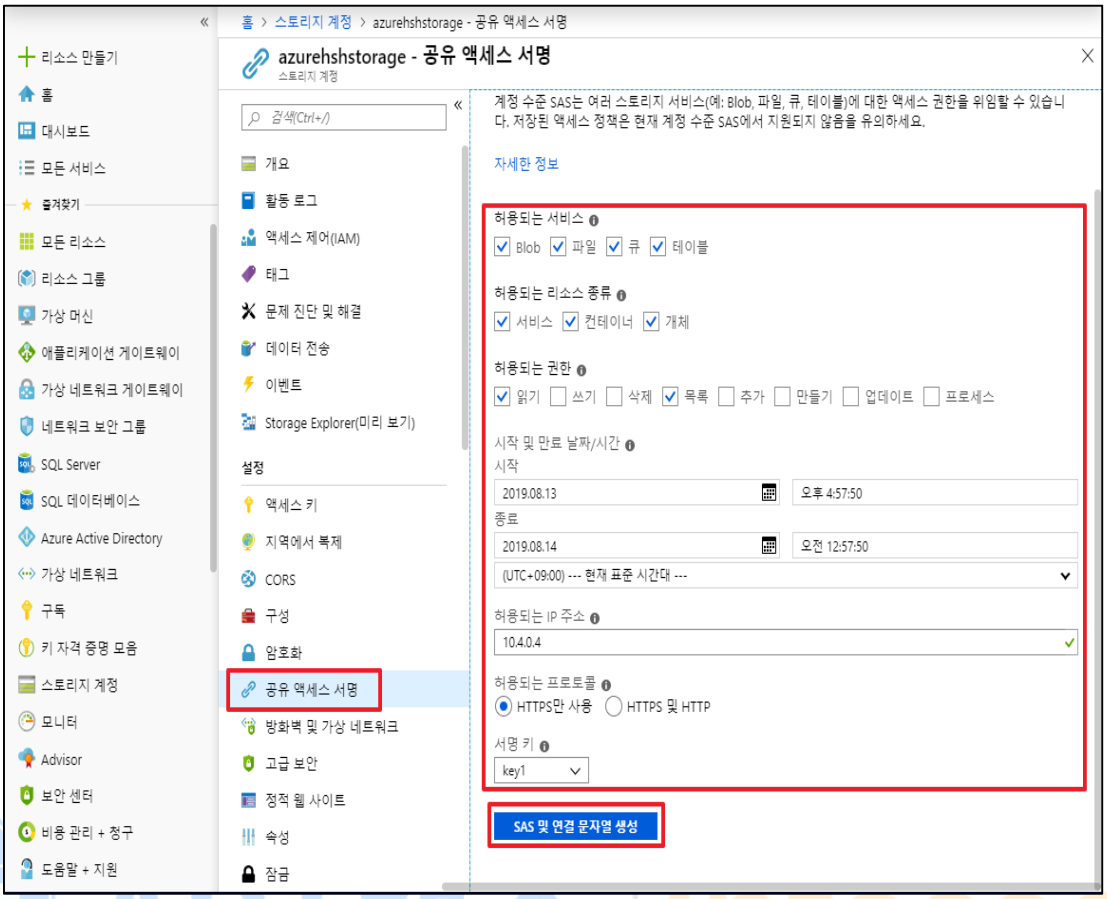
	취약기준 : IAM 의 사용자 및 권한에 맞게 발급된 스토리지 계정을 운영하고 있지 않을 경우
비고	

4.13 스토리지 계정 공유 액세스 서명 사용 관리

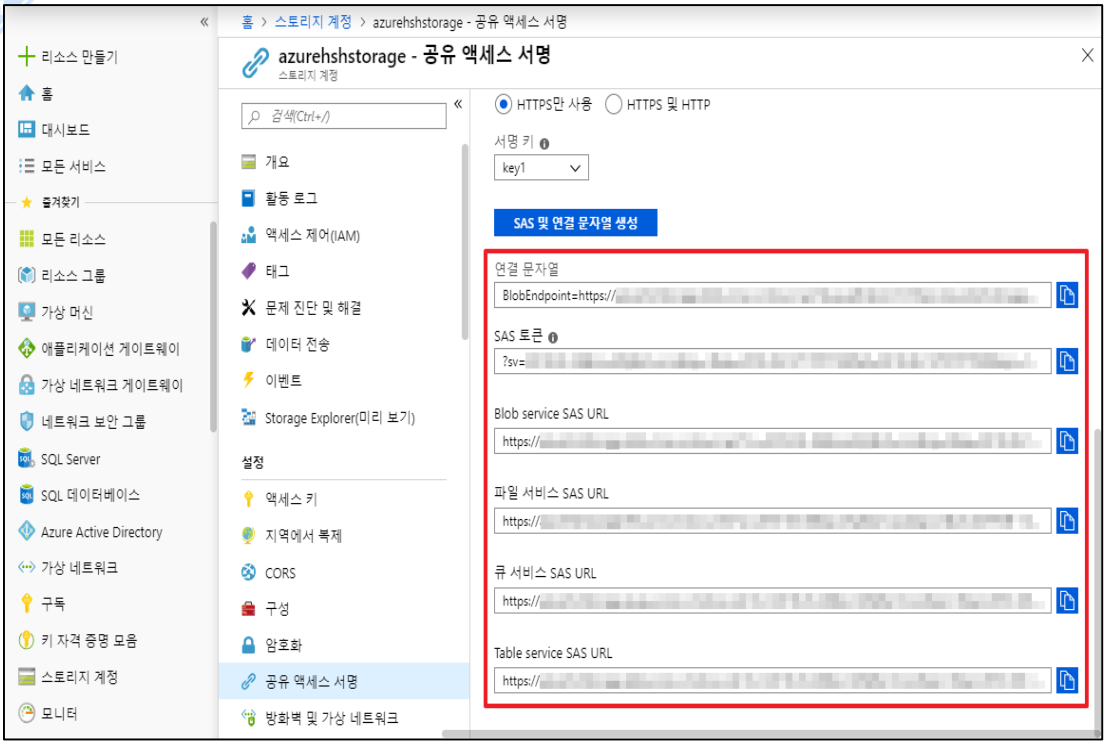
분류	가상 리소스 관리	중요도	상
항목명	스토리지 계정 공유 액세스 서명 사용 관리		
항목 설명	공유 액세스 서명은 하나 이상의 저장소 리소스를 가리키는 서명된 URI로, 특정 기간동안 저장소 계정의 리소스에 대한 위임된 권한을 제공합니다. SAS 토큰은 리소스 요청을 위해 필요한 정보가 포함되어 있으며, 액세스 가능한 서비스, 리소스, 사용 권한 및 서명이 유효한 시간 등으로 구성되어 있습니다. SAS 토큰이 유출될 경우 사용 권한이 없는 비인가자가 저장소 리소스에 액세스할 수 있으므로 필요하지 않을 경우 사용을 금지해야 합니다.		
설정 방법	**가. 가상 스토리지 공유 액세스 서명 (SAS) 설정 방법** 1) 스토리지 계정 메뉴 내 공유 액세스 서명을 생성할 스토리지 계정 선택  2) 구성 메뉴 내 공유 키 액세스 허용을 '사용 안 함' 설정 		
진단 기준	**양호기준** : 공유 액세스 서명을 사용하고 있지 않을 경우 **취약기준** : 공유 액세스 서명을 사용하고 있을 경우		
비고			

4.14 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 기간동안 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) 설정가능 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 생성여부 확인

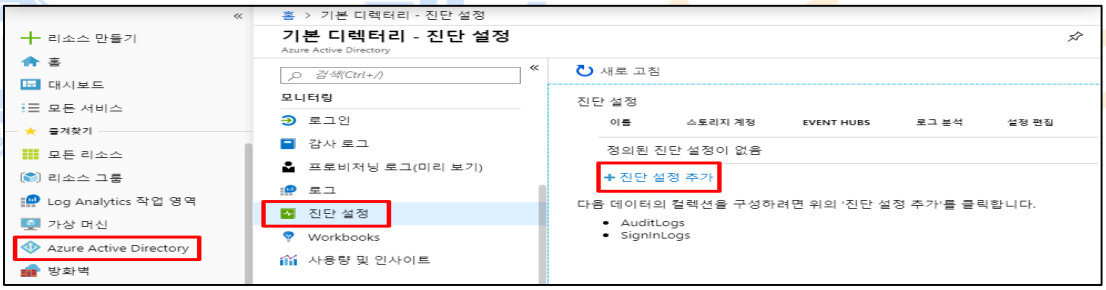
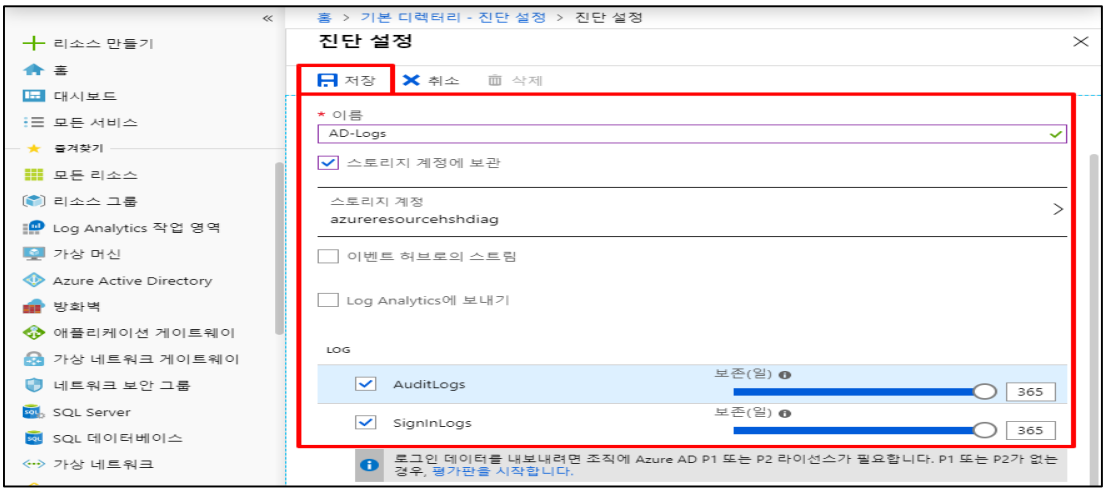


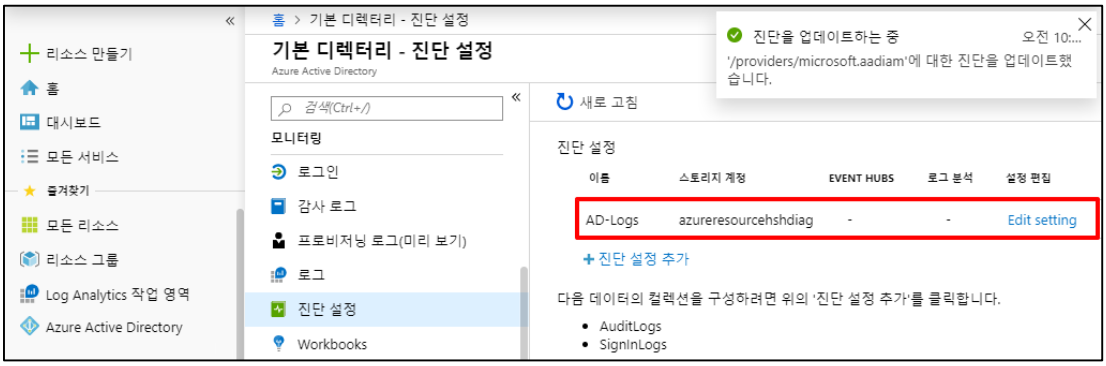
진단	양호기준

기준	: 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	

5. 감사추적

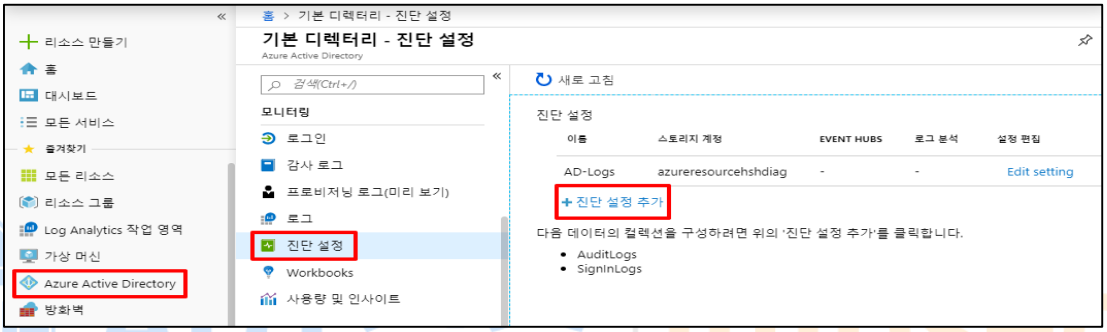
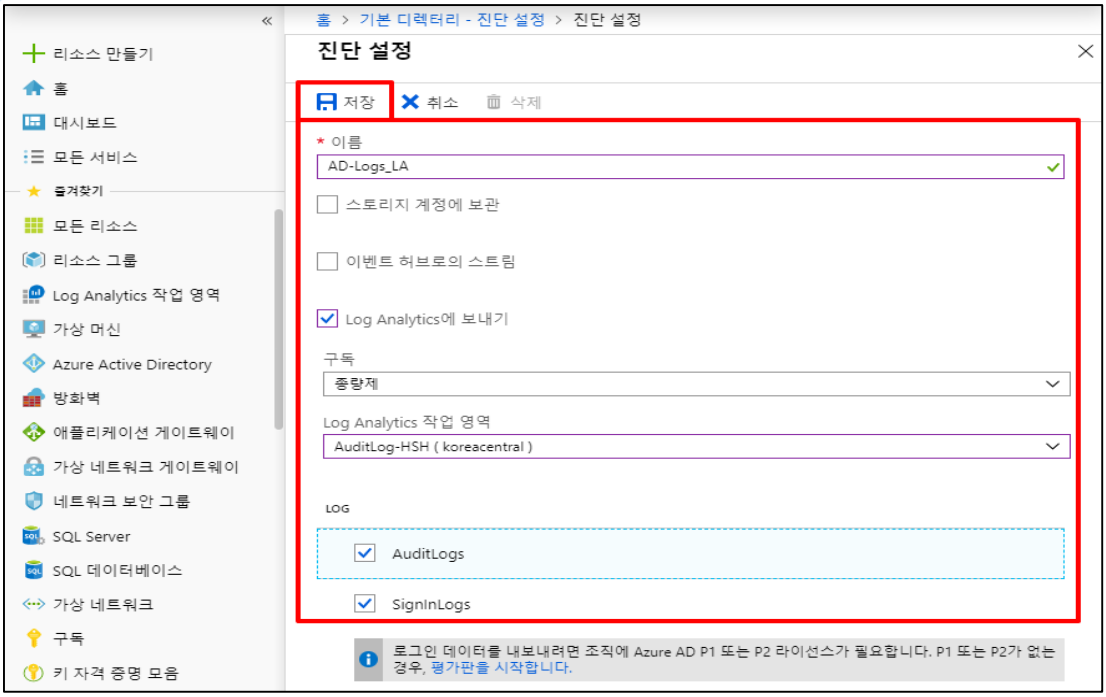
5.1 AD 감사 로그

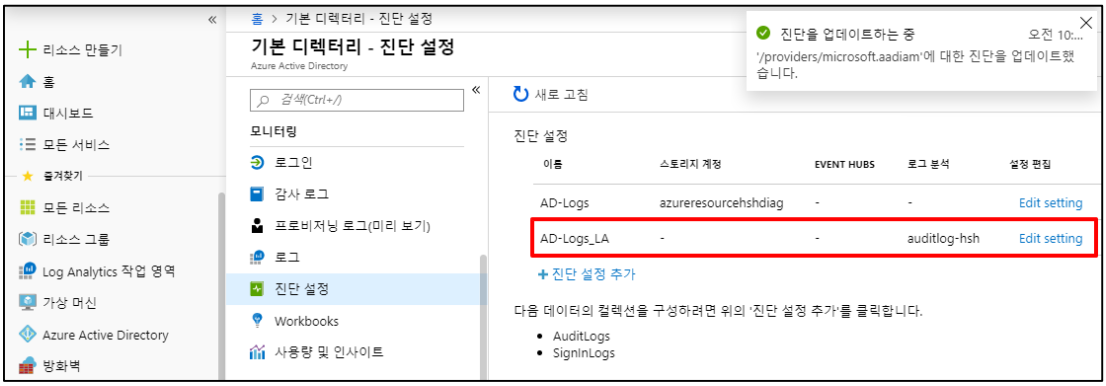
분류	감사/추적 관리	중요도	하
항목명	AD 감사 로그		
항목 설명	Azure AD 내의 다양한 기능에 의해 수행된 모든 변경내용에 대한 로그를 통해 추적기능을 제공합니다. 감사 로그의 예제로는 사용자, 앱, 그룹, 역할 및 정책 추가 또는 제거와 같은 Azure AD 내의 모든 리소스에 대한 변경 내용이 있습니다. 감사로그는 일반 사용자도 자신의 감사로그를 확인할 수 있으나, 게스트 계정은 별도 관리자 권한을 부여받지 않는 이상 감사로그를 확인할 수 없습니다. 기본적으로 제한적 권한을 갖는 게스트 사용자 계정은 최소권한으로 최소기간으로 사용되어야 하므로, 관리자 권한이 부여되지 않도록 주의해야 합니다. **※ AD 감사 로그는 최대 30 일간 저장되며, 더 긴 보존기간이 필요할 경우, 다운로드를 통해 별도 보관 및 관리하거나, 스토리지 계정으로 보관을 통해 별도관리가 필요합니다.**		
설정 방법	**가. Azure AD 감사로그 스토리지 저장 설정 방법** 1) Azure Active Directory 메뉴 내 진단 설정 및 진단설정 추가 버튼 선택  2) 진단 설정 기본 사항 값 설정 및 저장**(보존일수가 '0'일 경우 로그가 무기한 보존됨)**  3) 진단 설정 목록 내 정상 생성유무 확인		

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: AD 감사 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우

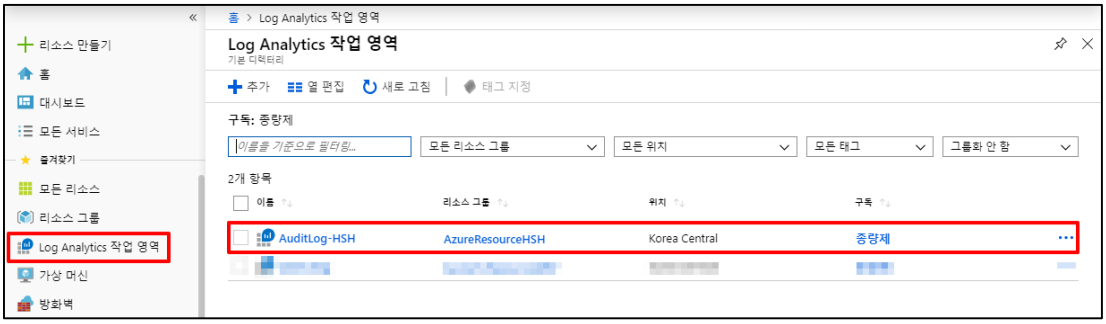
취약기준
: AD 감사 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

5.2 Azure 모니터 로그 통합 (Log Analytics)

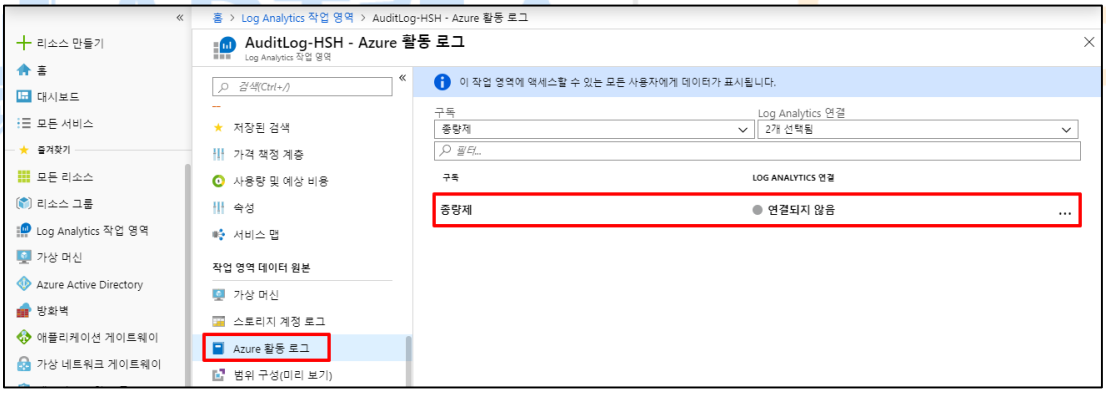
분류	감사/추적 관리	중요도	하
항목명	Azure 모니터 로그 통합 (Log Analytics)		
항목 설명	Azure AD(Active Directory)에서 발생하는 로그를 Log Analytics 보내기 기능을 통해 Azure 모니터 로그와 통합할 수 있고, 이를통해 로그 데이터를 검색, 쿼리, 시각화가 가능하며, 관련 경고 등의 작업이 가능합니다. **※ 지원 활동 보고서 종류** - 감사 로그(AuditLogs) : 태넌트에서 수행된 모든 작업의 기록에 액세스 가능 - 로그인 로그(SignInLogs) : 감사 로그에 보고된 작업을 수행한 사용자 확인 가능		
설정 방법	**가. Azure AD(Active Directory) 감사 및 활동 로그 설정 방법** 1) Active Directory 메뉴 내 진단 설정 및 진단 설정 추가 버튼 선택  2) 진단 설정 관련 기본 사항 값 설정 및 저장  3) 진단 설정 목록 내 정상 생성유무 확인		



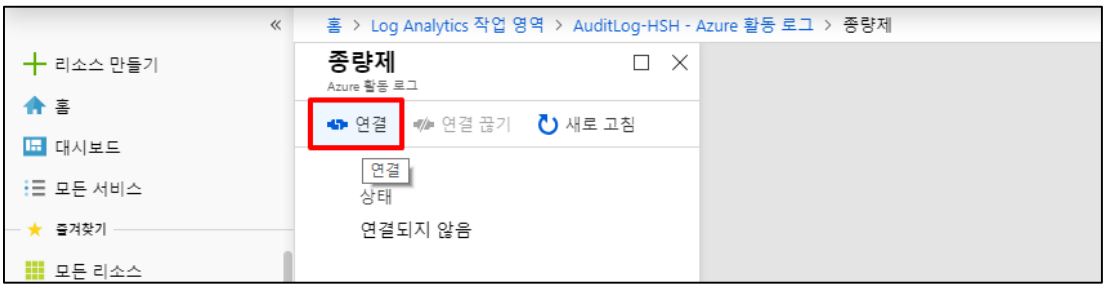
4) Log Analytics 작업 영역 메뉴 내 Azure 활동 로그를 설정할 Log Analytics 선택



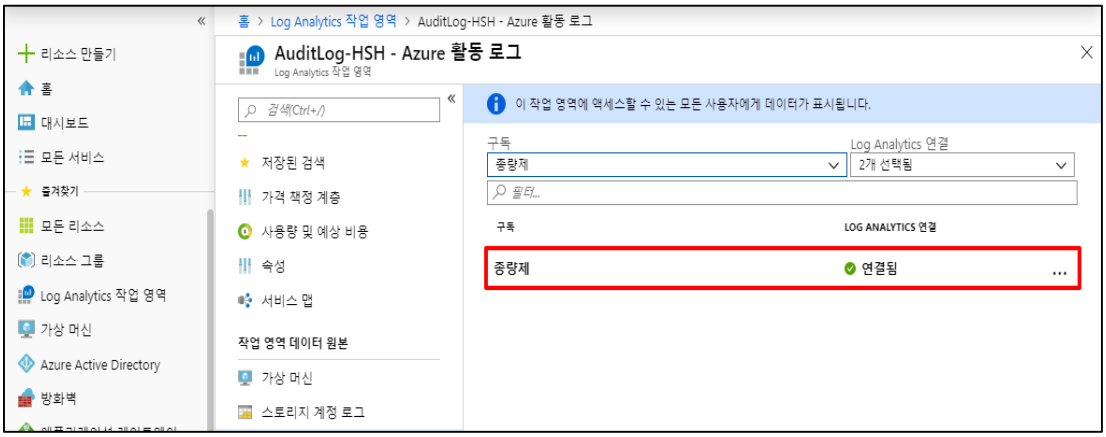
5) Azure 활동 로그 메뉴 내 구독 선택



6) 선택된 구독 메뉴 내 연결 버튼 선택



7) Azure 활동 로그 목록 내 정상 생성유무 확인

	
진단 기준	**양호기준** : 가상 리소스 모니터링 및 로그 설정이 되어 있을 경우 **취약기준** : 가상 리소스 모니터링 및 로그 설정이 되어 있지 않을 경우
비고	

2021 클라우드 보안 가이드 -Azure

ADT캡스 | infosec

경기도 성남시 분당구 판교로 227번길 23

발행인 : ADT캡스 취약점진단팀