

한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. LAB02B

Azure Policy를 통해 거버넌스 관리

이 문서는 Microsoft Technical Trainer팀에서 ESI 교육 참석자분들에게 제공해 드리는 문서입니다.

Microsoft Technical Trainer



요약

이 내용들은 표시된 날짜에 Microsoft에서 검토된 내용을 바탕으로 하고 있습니다. 따라서, 표기된 날짜 이후에 시장의 요구사항에 따라 달라질 수 있습니다. 이 문서는 고객에 대한 표기된 날짜 이후에 변화가 없다는 것을 보증하지 않습니다.

이 문서는 정보 제공을 목적으로 하며 어떠한 보증을 하지는 않습니다.

저작권에 관련된 법률을 준수하는 것은 고객의 역할이며, 이 문서를 마이크로소프트의 사전 동의 없이 어떤 형태(전자 문서, 물리적인 형태 막론하고) 어떠한 목적으로 재 생산, 저장 및 다시 전달하는 것은 허용되지 않습니다.

마이크로소프트는 이 문서에 들어있는 특허권, 상표, 저작권, 지적 재산권을 가집니다. 문서를 통해 명시적으로 허가된 경우가 아니면, 어떠한 경우에도 특허권, 상표, 저작권 및 지적 재산권은 다른 사용자에게 허용되지 않습니다.

© 2023 Microsoft Corporation All right reserved.

Microsoft®는 미합중국 및 여러 나라에 등록된 상표입니다.

이 문서에 기재된 실제 회사 이름 및 제품 이름은 각 소유자의 상표일 수 있습니다.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2021.11.17	1.0.0	우진환	LAB02B 작성
2022.10.03	1.1.0	우진환	Azure 포털 변경 사항 적용
2023.02.11	1.2.0	우진환	Cloudslice 변경 사항 적용
2023.05.30	1.3.0	우진환	Cloudslice 변경 사항 적용

목차

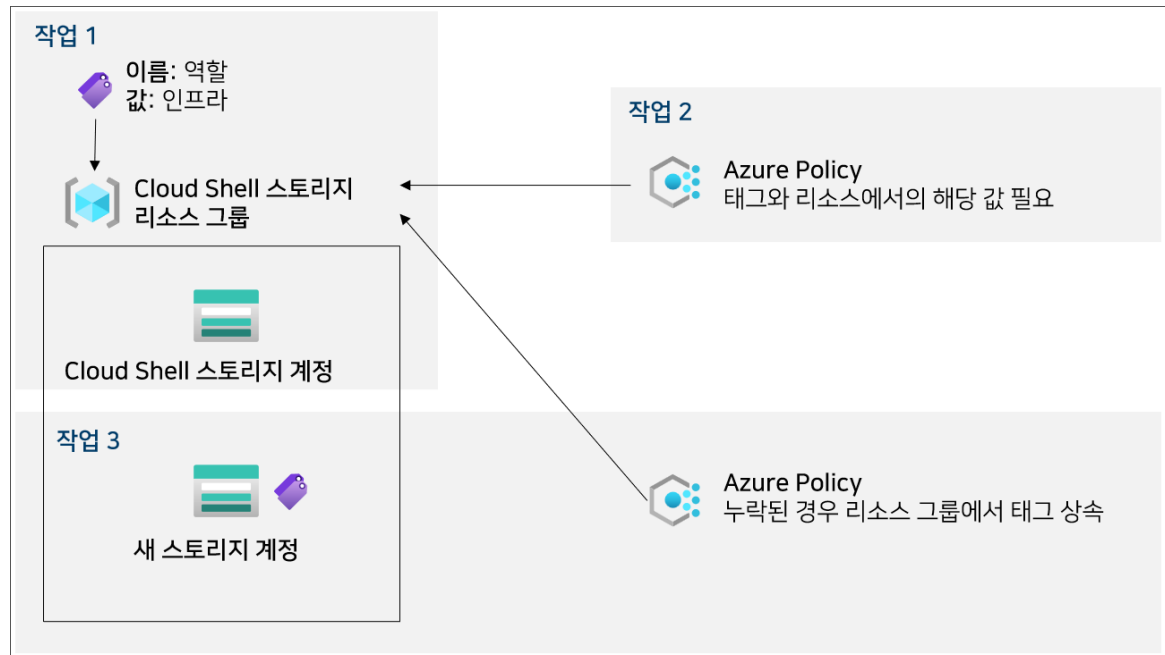
실습 시나리오	4
아키텍처 다이어그램	4
TASK 01. AZURE 포털을 통해 태그 할당	4
TASK 02. AZURE POLICY를 통해 태깅 적용	7
TASK 03. AZURE POLICY를 통해 태그 적용	10
TASK 04. 리소스 정리	14

실습 시나리오

Contoso의 Azure 리소스 관리를 개선하기 위해 다음 기능을 구현하는 업무를 맡게 되었습니다.

- 인프라 리소스만 포함하는 리소스 그룹을 태그 지정합니다.
- 적절하게 태그가 지정된 인프라 리소스만 인프라 리소스 그룹에 추가할 수 있도록 합니다.
- 모든 비준수 리소스를 수정합니다.

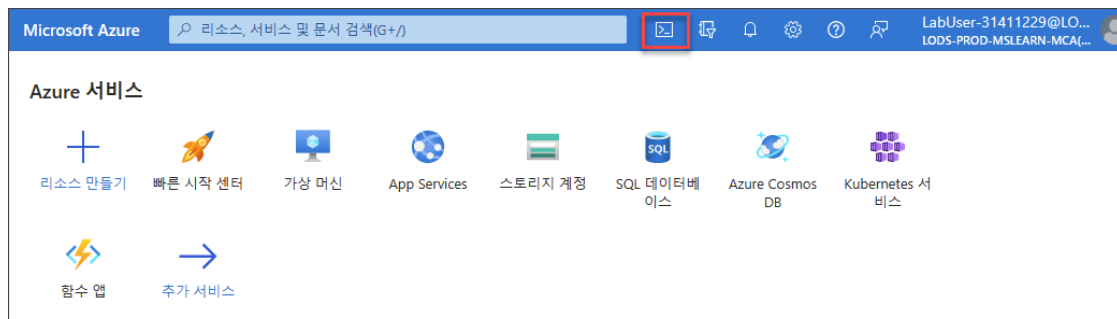
아키텍처 다이어그램



TASK 01. Azure 포털을 통해 태그 할당

이 작업에서는 Azure 포털을 통해 태그를 만들고 Azure 리소스 그룹에 태그를 할당합니다.

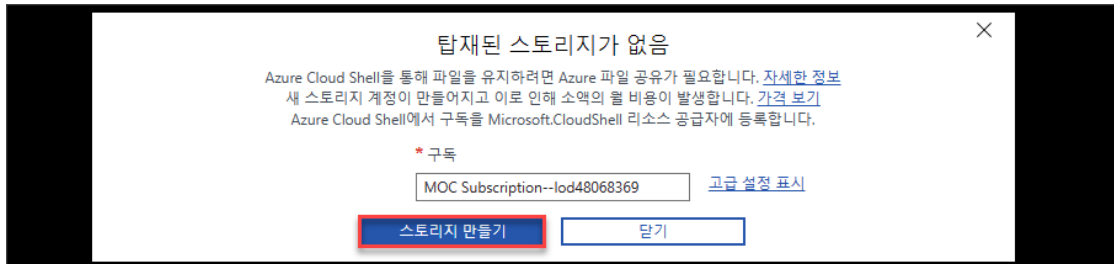
1. Azure 포털의 우측 상단 메뉴에서 [Cloud Shell] 아이콘을 클릭합니다.



2. [Azure Cloud Shell 시작] 창에서 "PowerShell"을 클릭합니다.

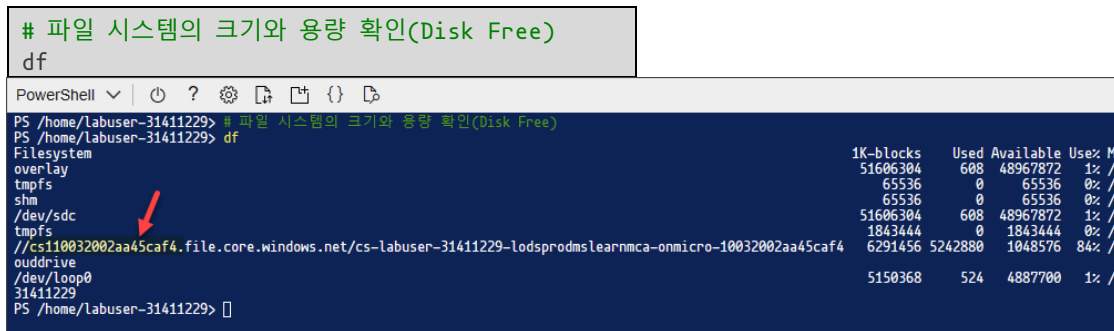


3. [탐재된 스토리지가 없음] 창에서 자신의 구독을 선택하고 [스토리지 만들기]를 클릭합니다.

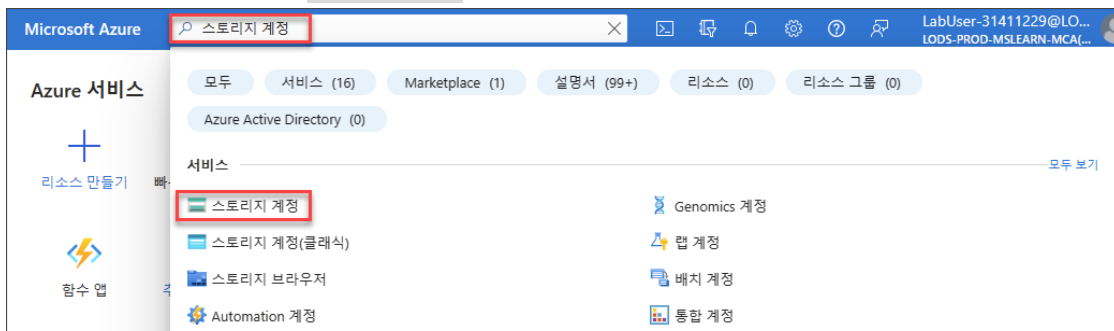


4. [Cloud Shell]에서 Cloud Shell이 사용하는 스토리지 계정의 이름을 확인하기 위해 다음 명령을 실행합니다.

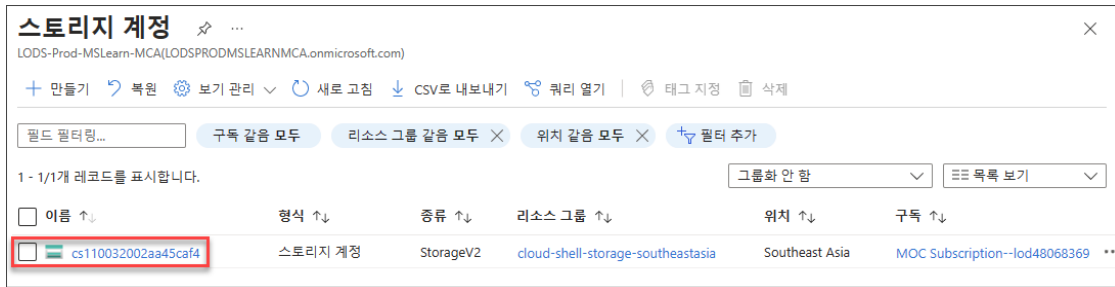
- 명령 출력에서 홈 드라이브(/usr/csuser/clouddrive) 마운트를 지정하는 정규화된 경로의 첫 번째 부분을 메모장에 기록합니다.
- 이 경로는 스토리지 계정의 파일 공유 경로입니다.



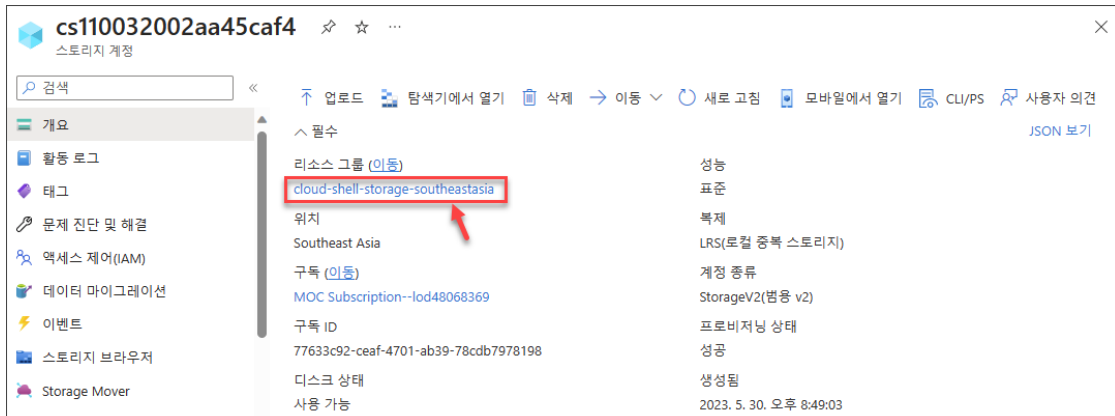
5. Azure 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다.



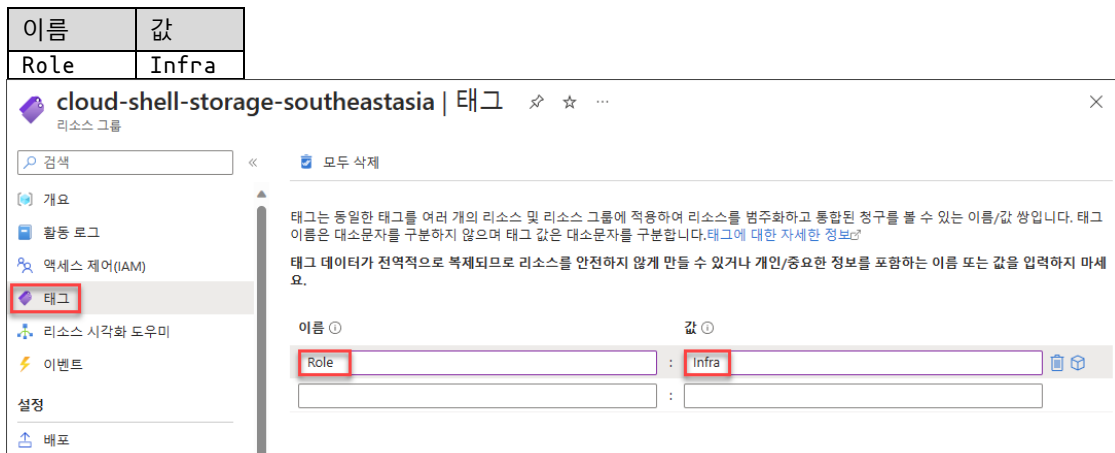
6. [스토리지 계정] 블레이드에서 위에서 확인했던 스토리지 이름을 클릭합니다.



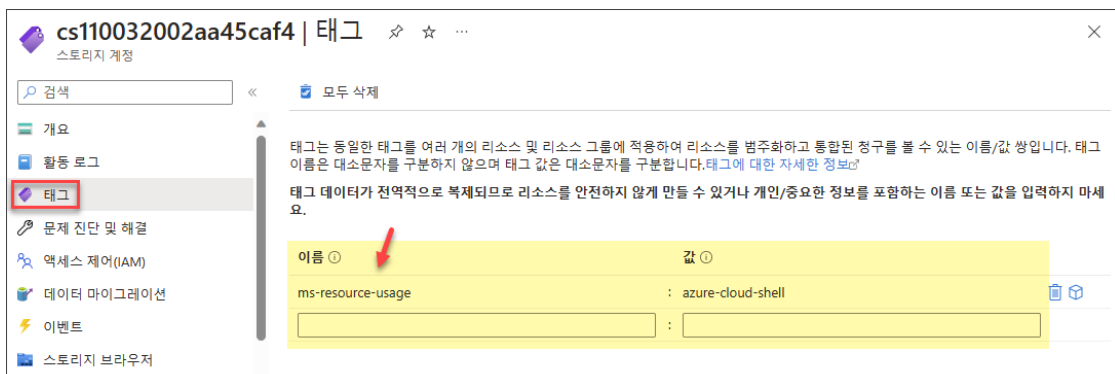
7. [스토리지 계정] 블레이드의 [개요]에서 리소스 그룹을 표시하는 링크를 클릭합니다.



8. [리소스 그룹] 블레이드의 [태그]로 이동한 후 다음과 같은 태그를 추가하고 [적용]을 클릭합니다.



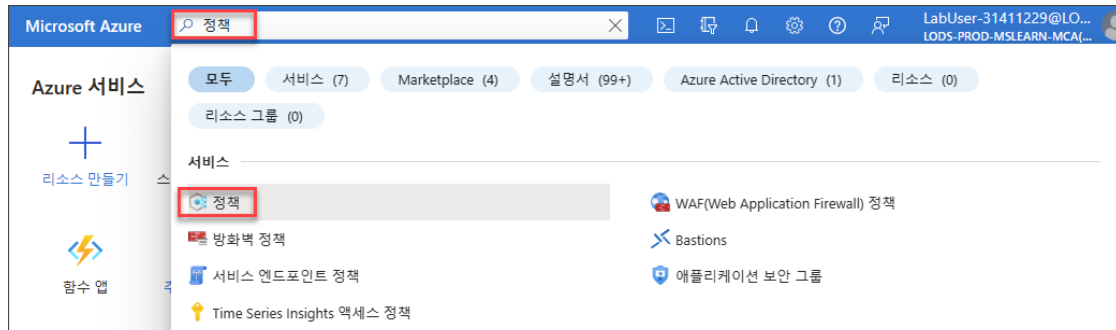
9. [스토리지 계정] 블레이드로 이동한 후 [태그]를 클릭합니다. 리소스 그룹에 설정한 태그가 스토리지 계정에 자동으로 할당되지 않은 것을 확인합니다.



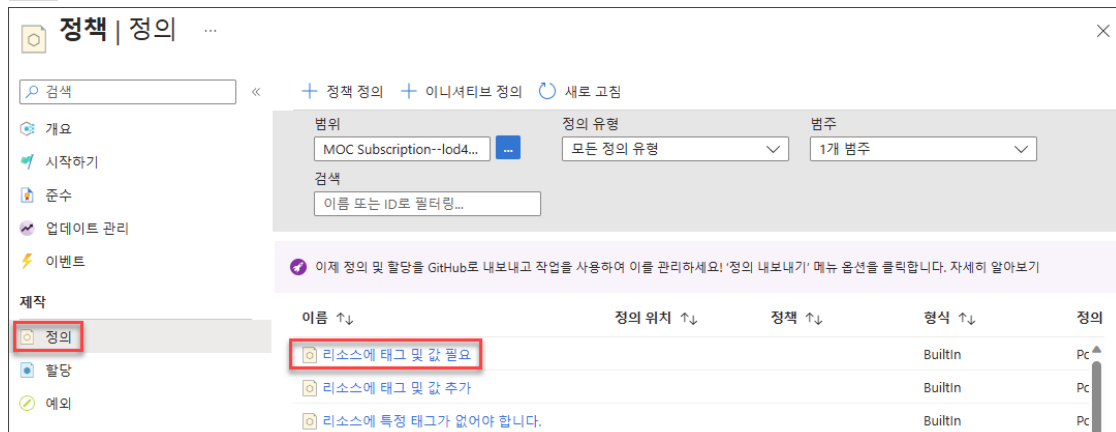
TASK 02. Azure Policy를 통해 태깅 적용

이 작업에서는 "리소스에 태그 및 값 필요" 빌트인 정책을 리소스 그룹에 할당하고 결과를 평가합니다.

1. Azure 포털의 검색창에서 "정책"을 검색한 후 [정책]을 클릭합니다.



2. [정책] 블레이드의 [제작 - 정의]로 이동합니다. 범주를 "Tags"로 선택한 후 "리소스에 태그 및 값 필요" 정책을 클릭합니다.



3. [리소스에 태그 및 값 필요] 블레이드의 메뉴에서 [할당]을 클릭합니다.



4. [리소스에 태그 및 값 필요] 페이지의 [기본 내용] 탭에서 "범위"의 [...]을 클릭합니다. [범위] 창에서 자신의 구독과 Cloud Shell의 스토리지 계정을 포함하고 있는 리소스 그룹을 선택하고 [선택]을 클릭합니다.

- 범위는 정책 할당이 적용되는 리소스 혹은 리소스 그룹을 결정합니다.
- 관리 그룹, 구독 혹은 리소스 그룹 수준에 정책을 할당할 수 있으며 개별 구독, 리소스 그룹 혹은 리소스와 같은 제외를 지정하는 옵션도 있습니다.

리소스에 태그 및 값 필요 ...

정책 할당

기본 내용 고급 매개 변수 재구성 미준수 메시지 검토 + 만들기

범위

범위 범위 설정에 대한 자세한 정보 *

구독 MOC Subscription--lod48068369

리소스 그룹 cloud-shell-storage-southeastasia

제외

정책 할당에서 제외할 리소스를 선택적으로 선택합니다.

5. [리소스에 태그 및 값 필요] 페이지의 [기본 내용] 탭에서 다른 값을 다음과 같이 지정한 후 [매개 변수] 탭을 클릭합니다.

- 할당 이름: Require Role tag with Infra value
- 설명: Require Role tag with Infra value for all resources in the Cloud Shell resource group
- 정책 적용: 사용

리소스에 태그 및 값 필요 ...

정책 할당

기본 내용 고급 매개 변수 재구성 미준수 메시지 검토 + 만들기

범위

범위 범위 설정에 대한 자세한 정보 *

MOC Subscription--lod48068369/cloud-shell-storage-southeastasia

제외

정책 할당에서 제외할 리소스를 선택적으로 선택합니다.

기본 내용

정책 정의

리소스에 태그 및 값 필요

할당 이름 * ①

Require Role tag with infra value

설명

Require Role tag with Infra value for all resources in the Cloud Shell resource group

정책 적용 ①

사용 사용 안 함

6. [매개 변수] 탭에서 다음과 같이 구성하고 [다음]을 클릭합니다.

- 태그 이름: Role
- 태그 값: Infra

리소스에 태그 및 값 필요 ...

정책 할당

기본 내용 고급 매개 변수 재구성 미준수 메시지 검토 + 만들기

매개 변수 이름...

☒ 입력 또는 검토가 필요한 매개 변수만 표시

태그 이름 * ①

Role

태그 값 * ①

Infra

7. [재구성] 탭에서 기본값을 유지하고 [검토 + 만들기]를 클릭합니다. 이 설정은 정책 혹은 이니셔티브가 `deployIfNotExists` 및 `Modify` 효과를 포함하고 있는 경우에 사용됩니다.

리소스에 태그 및 값 필요 ...

정책 할당

기본 내용 고급 매개 변수 **재구성** 미준수 메시지 검토 + 만들기

기본적으로 이 할당은 새로 만든 리소스에만 적용됩니다. 정책이 할당된 후에 수정 작업을 통해 기존 리소스를 업데이트할 수 있습니다. deployIfNotExists 정책의 경우 수정 작업에서 지정된 템플릿을 배포합니다. 정책 수정의 경우 수정 작업에서 기존 리소스의 태그를 편집합니다.

관리 ID
 deployIfNotExists 및 수정 효과 유형이 있는 정책에는 각각 리소스를 배포하고 기존 리소스에 대한 태그를 편집하는 기능이 필요합니다. 이를 위해서는 기존 사용자 할당 관리 ID 또는 시스템 할당 관리 ID 생성 중에서 선택합니다.
[관리 ID에 대해 자세히 알아보세요.](#)

☐ 관리 ID 생성 ①

권한
 ⚠ 이 정책은 역할 정의를 포함하지 않습니다. 관리형 ID에 대해 올바른 역할 할당을 만들려면 deployIfNotExists 및 modify 정책이 역할 정의를 지정해야 합니다.

8. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다. 정책이 적용될 때까지 5~15분 정도 걸릴 수 있습니다.
9. 이제 필요한 태그를 명시적으로 추가하지 않고 리소스 그룹에 다른 스토리지 계정을 만들어 새 정책 할당이 적용되는지 확인합니다. 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다. [스토리지 계정] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

스토리지 계정 ...

LODS-Prod-MSLearn-MCA(LODSPRODMSLEARNMCA.onmicrosoft.com)

+ 만들기 🔍 복원 ⚙ 보기 관리 ▼ 🔄 새로 고침 ⬇ CSV로 내보내기 🔄 쿼리 열기 | 🏷 태그 지정 🗑 삭제

필터 필터링... 그룹 다음 모두 리소스 그룹 다음 모두 × 위치 다음 모두 × 📌 필터 추가

1 - 1/1개 레코드를 표시합니다. 그룹화 안 함 목록 보기

<input type="checkbox"/> 이름 ↑↓	형식 ↑↓	종류 ↑↓	리소스 그룹 ↑↓	위치 ↑↓	구독 ↑↓
<input type="checkbox"/> cs110032002aa45caf4	스토리지 계정	StorageV2	cloud-shell-storage-southeastasia	Southeast Asia	MOC Subscription--lod48068369

10. [저장소 계정 만들기] 페이지의 [기본] 탭에서 다음과 같이 구성한 후 [검토]를 클릭합니다. [검토] 탭에서 [만들기]를 클릭합니다.
 - [프로젝트 정보 - 리소스 그룹]: Cloud Shell용 스토리지 계정을 포함하고 있는 리소스 그룹을 선택합니다.
 - [인스턴스 정보 - 스토리지 계정 이름]: labuser<xxxxxxxx>
 - [인스턴스 정보 - 지역]: (US) East US
 - [인스턴스 정보 - 성능]: 표준
 - [인스턴스 정보 - 중복]: GRS(지역 중복 스토리지)

저장소 계정 만들기 ...

기본 고급 네트워크 데이터 보호 암호화 태그 검토

Azure Storage는 가용성, 보안, 내구성, 확장성 및 중복성이 뛰어난 클라우드 스토리지를 제공하는 Microsoft 관리 서비스입니다. Azure Storage는 Azure Blob(개체), Azure Data Lake Storage Gen2, Azure Files, Azure 큐 및 Azure 테이블을 포함합니다. 스토리지 계정의 비용은 사용량 및 아래에서 선택한 옵션에 따라 다릅니다. [Azure Storage 계정에 대한 자세한 정보](#)

프로젝트 정보
새 스토리지 계정을 만들 구독을 선택합니다. 다른 리소스와 함께 스토리지 계정을 구성하고 관리할 새 리소스 그룹 또는 기존 리소스 그룹을 선택합니다.

구독 * MOC Subscription--lod48068369
리소스 그룹 * cloud-shell-storage-southeastasia
[새로 만들기](#)

인스턴스 정보
레거시 스토리지 계정 유형을 생성해야 하는 경우 여기를(를) 클릭하세요.

스토리지 계정 이름 * labuser31411229
지역 * (US) East US
[여기 영역에 배포](#)

성능 *
☒ 표준: 대부분 시나리오에 권장됨(범용 v2 계정)
☐ 프리미엄: 짧은 대기 시간이 필요한 경우에 권장됩니다.

중복 * GRS(지역 중복 스토리지)
☒ 지역 가용성이 없는 경우에 사용할 수 있는 데이터의 읽기 권한을 만듭니다.

11. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다. 아래와 같이 배포 오류가 표시됩니다. 배포 오류 링크를 클릭하면 앞서 만들었던 Azure Policy인 "Require Role tag with Infra value" 정책 위반으로 인해 배포가 실패한 것을 확인할 수 있습니다.

오류

요약 Raw 오류

오류 정보

정책에서 'labuser31411229' 리소스를 허용하지 않았습니다. (코드: RequestDisallowedByPolicy)

정책: Require Role tag with Infra value

이 정보가 도움이 되었나요? [👍](#) [👎](#)

문제 해결 옵션

- [일반적인 Azure 배포 오류](#)
- [사용량 + 할당량 확인](#)
- [새 지원 요청](#)

TASK 03. Azure Policy를 통해 태그 적용

이 작업에서는 다른 정책 정의를 사용하여 비준수 리소스를 수정합니다.

1. Azure 포털의 검색창에서 "정책"을 검색한 후 클릭합니다.

Microsoft Azure

검색창: 정책

Azure 서비스

리소스 만들기

리소스 그룹 (0)

서비스

정책

방화벽 정책

서비스 엔드포인트 정책

Time Series Insights 액세스 정책

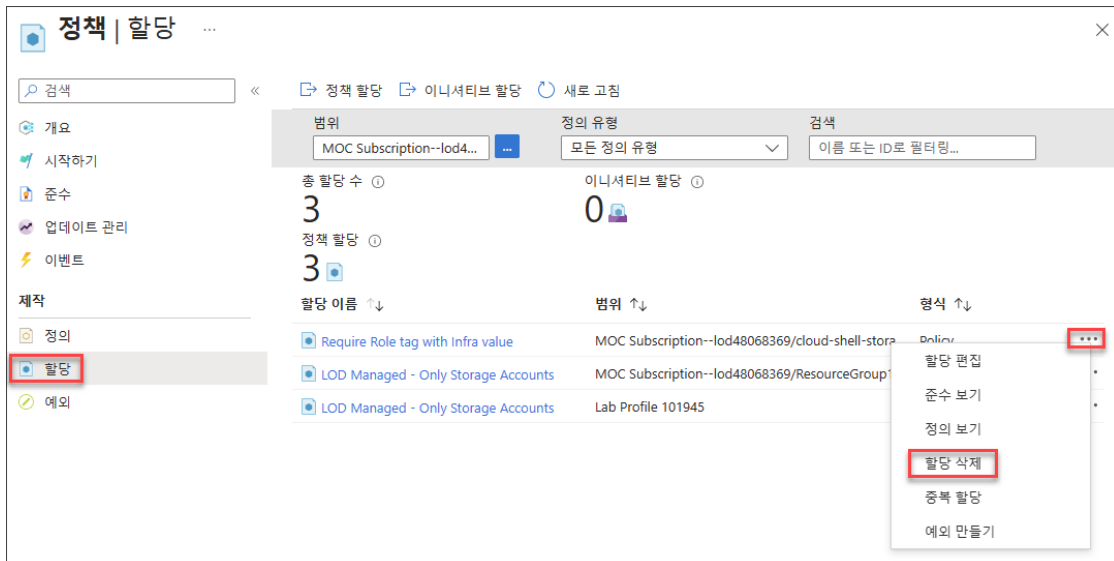
WAF(Web Application Firewall) 정책

Bastions

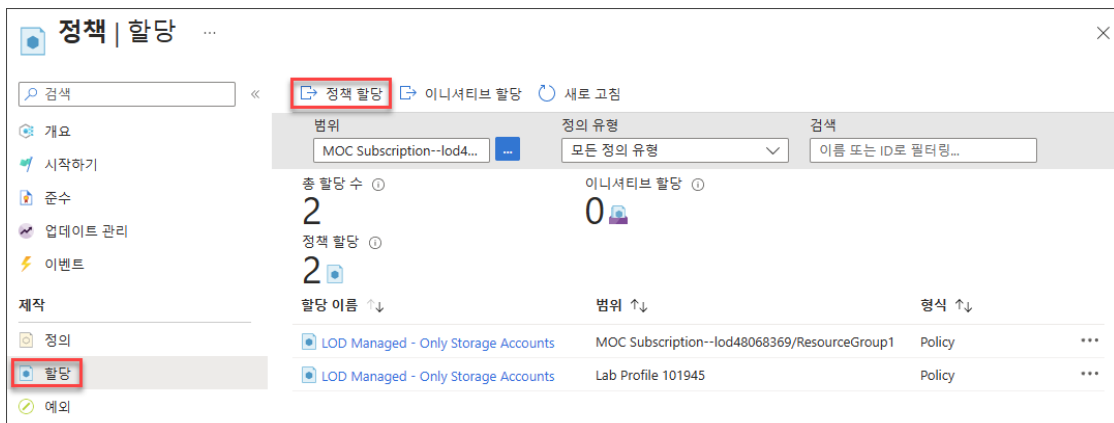
애플리케이션 보안 그룹

2. [정책] 블레이드의 [제작 - 할당]으로 이동한 후 "Require Role tag with Infra value" 정책의

[... - 할당 삭제]를 클릭합니다. [할당 삭제] 창에서 [예]를 클릭합니다.



3. [정책] 블레이드의 [제작 - 할당]에서 [정책 할당]을 클릭합니다.



4. [정책 할당] 페이지의 [기본 내용] 탭에서 아래와 같이 구성한 후 [매개 변수] 탭을 클릭합니다.

- [범위 - 범위]: [...]을 클릭한 후 자신의 구독과 Cloud Shell의 스토리지 계정이 포함되어 있는 리소스 그룹을 선택합니다.
- [기본 내용 - 정책 정의]: [...]을 클릭한 후 "없는 경우 리소스 그룹에서 태그 상속"을 선택합니다.
- [기본 내용 - 할당 이름]: Inherit the Role tag and its Infra value from the Cloud Shell resource group if missing
- [기본 내용 - 설명]: Inherit the Role tag and its Infra value from the Cloud Shell resource group if missing
- [기본 내용 - 정책 적용]: 사용

정책 할당 ...

기본 내용 고급 매개 변수 재구성 미준수 메시지 검토 + 만들기

범위
범위 범위 설정에 대한 자세한 정보 *

MOC Subscription--lod48068369/cloud-shell-storage-southeastasia ✓ ...

제외
정책 할당에서 제외할 리소스를 선택적으로 선택합니다. ...

기본 내용
정책 정의 *

없는 경우 리소스 그룹에서 태그 상속 ✓ ...

할당 이름 * ①
Inherit the Role tag and its infra value from the Cloud Shell resource group if missing ✓

설명
Inherit the Role tag and its infra value from the Cloud Shell resource group if missing

정책 적용 ①
☒ 사용 ☐ 사용 안 함

할당한 사람

5. [매개 변수] 탭에서 태그 이름에 "Role"을 입력하고 [다음]을 클릭합니다.

정책 할당 ...

기본 내용 고급 매개 변수 재구성 미준수 메시지 검토 + 만들기

매개 변수 이름으... ☒ 입력 또는 검토가 필요한 매개 변수만 표시

태그 이름 * ①
Role ✓

6. [재구성] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. 이 정책은 **Modify** 효과를 포함하고 있기 때문에 관리 ID (Managed Identity)가 생성됩니다.

- "수정 작업 만들기" 옵션을 체크합니다.
- 수정할 정책: 없는 경우 리소스 그룹에서 태그 상속

정책 할당 ...

기본 내용 고급 매개 변수 **재구성** 미준수 메시지 검토 + 만들기

기본적으로 이 할당은 새로 만든 리소스에만 적용됩니다. 정책이 할당된 후에 수정 작업을 통해 기존 리소스를 업데이트할 수 있습니다. deployIfNotExists 정책의 경우 수정 작업에서 지정된 템플릿을 배포합니다. 정책 수정의 경우 수정 작업에서 기존 리소스의 태그를 편집합니다.

☒ 수정 작업 만들기 ①

수정할 정책
없는 경우 리소스 그룹에서 태그 상속

관리 ID
deployIfNotExists 및 수정 효과 유형이 있는 정책에는 각각 리소스를 배포하고 기존 리소스에 대한 태그를 편집하는 기능이 필요합니다. 이를 위해서는 기존 사용자 할당 관리 ID 또는 시스템 할당 관리 ID 생성 중에서 선택합니다.
[관리 ID에 대해 자세히 알아보세요.](#)

☒ 관리 ID 생성 ①

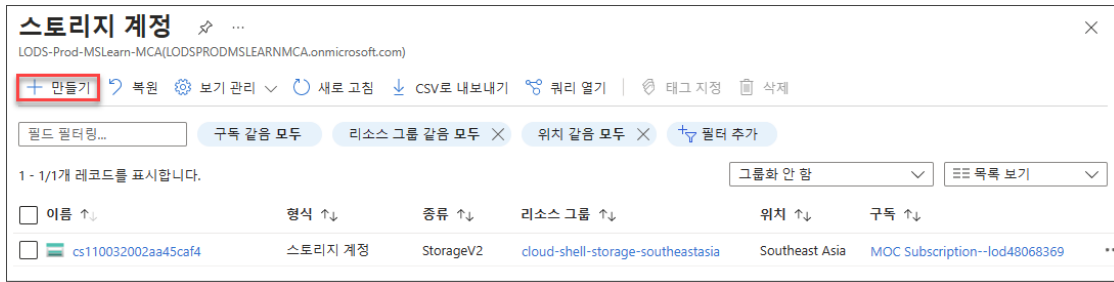
관리 ID 유형 ①
☒ 시스템이 할당한 관리 ID ☐ 사용자가 할당한 관리 ID

시스템 할당 ID 위치 *
East US

권한
이 ID에는 다음 권한도 부여됩니다.
기여자

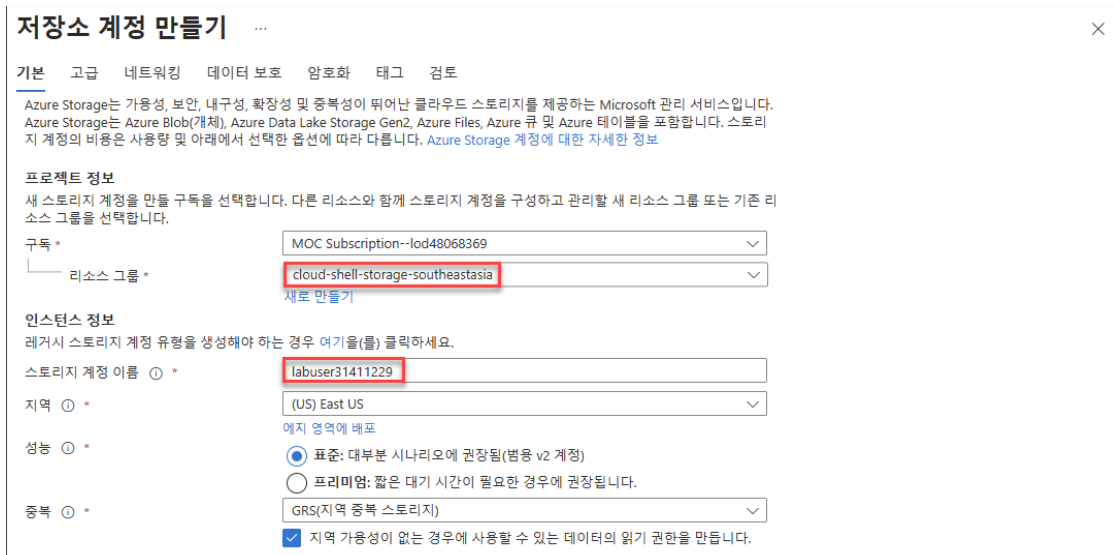
① 역할 할당(권한)은 정책에 지정된 역할 정의를 기반으로 생성됩니다.

7. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
8. 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다. [스토리지 계정] 블레이드의 메뉴에서 [만들기]를 클릭합니다.



9. [저장소 계정 만들기] 페이지의 [기본] 탭에서 다음과 같이 구성한 후 [검토]를 클릭합니다.

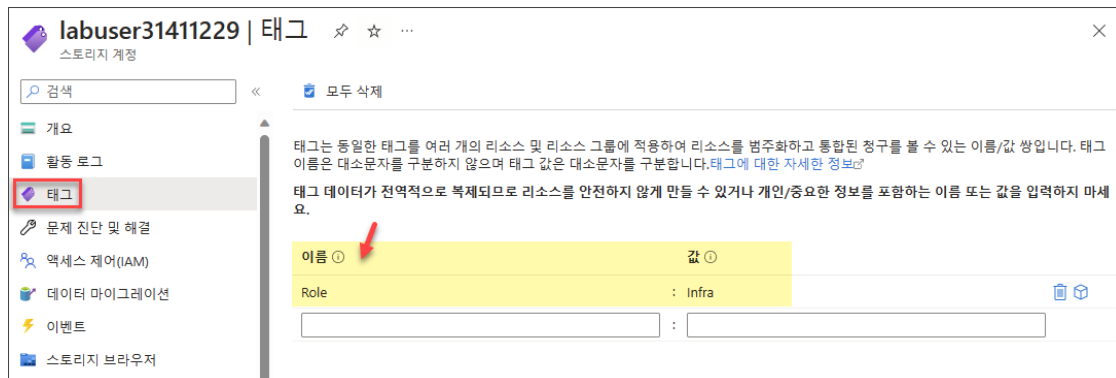
- [프로젝트 정보 - 리소스 그룹]: Cloud Shell의 스토리지 계정이 배포된 리소스 그룹이 선택되어 있는지 확인합니다.
- [인스턴스 정보 - 스토리지 계정 이름]: labuser<xxxxxxxx>
- [인스턴스 정보 - 지역]: (US) East US
- [인스턴스 정보 - 성능]: 표준
- [인스턴스 정보 - 중복]: GRS(지역 중복 스토리지)



10. [검토] 탭에서 [만들기]를 클릭합니다. 만약 이전과 마찬가지로 유효성 검사가 실패한다면 이전 정책을 삭제한 내용이 아직 적용되지 않은 것이므로 5~15분 정도 기다린 후 다시 스토리지 계정을 생성합니다. 배포가 완료되면 [리소스로 이동]을 클릭합니다.

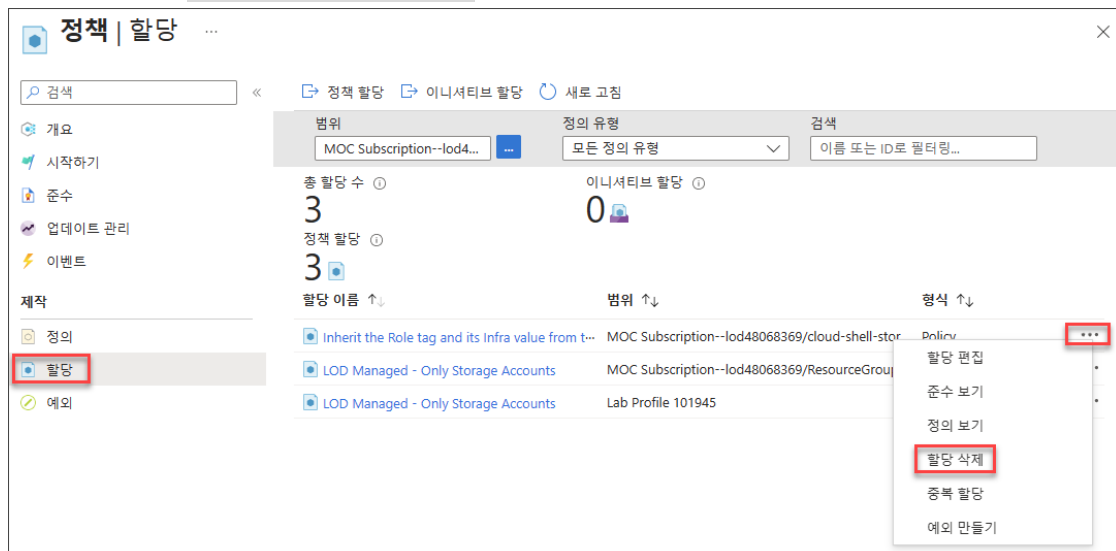


11. 새로 만든 [스토리지 계정] 블레이드의 [태그]로 이동한 후 정책을 통해 적용된 태그가 표시되는 것을 확인합니다.

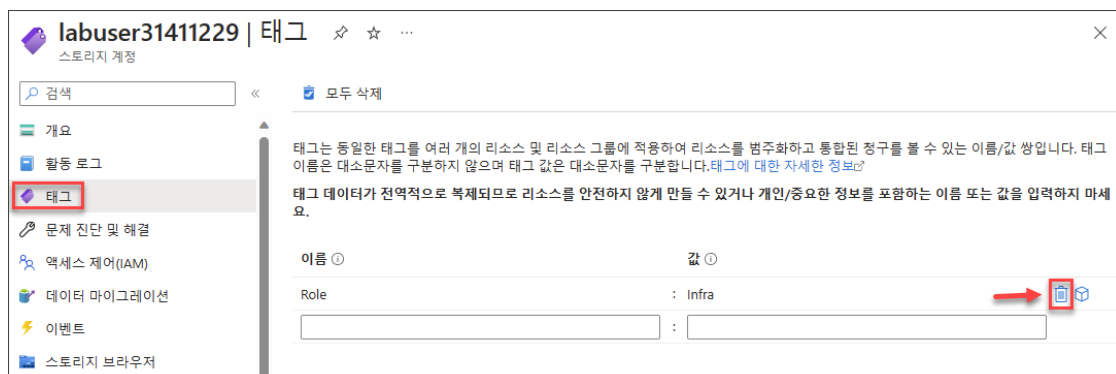


TASK 04. 리소스 정리

1. 포털의 검색창에서 "정책"을 검색한 후 클릭합니다. [정책] 블레이드의 [제작 - 할당]으로 이동한 후 앞서 만들었던 "Inherit the Role tag..." 정책의 [... - 할당 삭제]를 클릭하여 정책을 삭제합니다.



2. Azure 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다. 앞서 만든 labuser<xxxxxxxx> 스토리지 계정을 클릭합니다. [labuser<xxxxxxxx> 스토리지 계정] 블레이드의 [태그]로 이동한 후 수동으로 추가했던 태그의 [삭제] 아이콘을 클릭하여 태그를 삭제하고 [적용]을 클릭합니다.



3. 정책 테스트를 위해 만들었던 스토리지 계정 블레이드로 이동합니다. [스토리지 계정] 블레이드의 메뉴에서 [삭제]를 클릭합니다.



4. [스토리지 계정 삭제] 페이지에서 스토리지 계정 이름을 입력하고 [삭제]를 클릭합니다.

