

한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. Challenge Lab 03

LAB 01. Azure Web App을 위한 보안 구현

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

Microsoft Partner Program – Technical Advisory Service



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
2023.08.26	1.0.0	우진환	LAB 01 내용 작성

목차

도전 과제	4
STEP 01. RBAC을 사용하여 계정 보안 구성.....	4
STEP 02. 개발자 계정으로 웹 앱 만들기.....	4
STEP 03. 웹 앱과 가상 네트워크 통합.....	4
TASK 01. RBAC을 사용하여 계정 보안 구성	5
TASK 02. 개발자 계정으로 웹 앱 만들기	8
TASK 03. 웹 앱과 가상 네트워크 통합	11

도전 과제

이 실습에서는 개발자가 보안 웹 앱을 만들 수 있도록 합니다.

- RBAC을 사용하여 계정에 대한 보안을 구성합니다.
- 웹 앱을 만듭니다.
- 새 가상 네트워크를 만들고 웹 앱을 가상 네트워크에 통합합니다.

STEP 01. RBAC을 사용하여 계정 보안 구성

1. Dev-`<xxxxxxxx>` 계정이 RG1lod`<xxxxxxxx>` 리소스 그룹에 "웹 사이트 참가자(Website Contributor)", "웹 플랜 참가자(Web Plan Contributor)", "네트워크 참가자(Network Contributor)", "Storage 계정 참가자(Storage Account Contributor)" 권한을 가지도록 구성합니다.
2. Azure 포털에 Dev-`<xxxxxxxx>` 계정으로 로그인합니다.
3. RG1lod`<xxxxxxxx>` 리소스 그룹에 기본 설정을 사용하여 sa`<xxxxxxxx>` 이름의 스토리지 계정을 만듭니다.

STEP 02. 개발자 계정으로 웹 앱 만들기

1. Dev-`<xxxxxxxx>` 계정으로 다음 값을 사용하여 새 웹 앱을 만듭니다.

속성	값
리소스 그룹	RG1lod <code><xxxxxxxx></code>
이름	MyWebApp- <code><xxxxxxxx></code>
런타임 스택	ASP.NET V4.8
운영 체제	Windows
지역	East US
Windows 플랜 (East US)	AppPlan1
가격 책정 플랜	표준 S1

2. 새로 만든 웹 앱에 사용자 이름(ftp`<xxxxxxxx>`)과 암호(Pa55w.rd1234)를 사용하여 FTPS 자격 증명을 만듭니다.
3. 다음과 같은 외부 Git 리포지토리의 소스 코드를 사용하도록 웹 앱 배포를 설정합니다.
 - 리포지토리: https://github.com/L0DSContent/L0DS0C_app-service-web-dotnet-get-started
 - 브랜치: main
4. 배포된 웹 사이트를 확인합니다.

STEP 03. 웹 앱과 가상 네트워크 통합

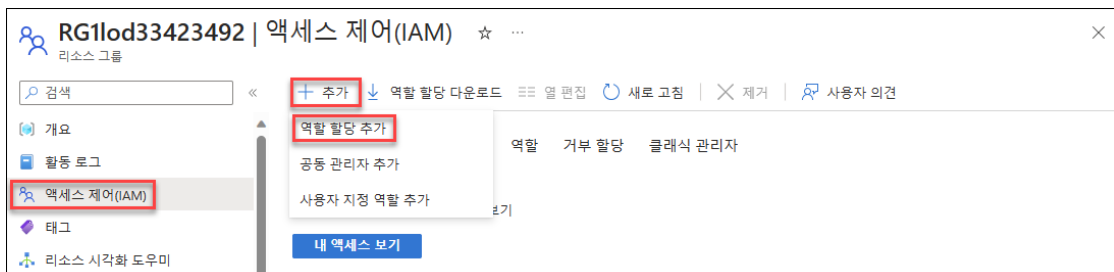
1. Dev-`<xxxxxxxx>` 계정으로 로그인 한 후 RG1lod`<xxxxxxxx>` 리소스 그룹에 VNET-`<xxxxxxxx>` 이름의 가상 네트워크를 만듭니다. IP 주소 공간을 포함한 다른 모든 설정은 기본 설정을 사용합니다.
2. 기본 서브넷을 사용하여 웹 앱을 새로 만든 가상 네트워크에 통합합니다.

TASK 01. RBAC을 사용하여 계정 보안 구성

1. Azure 포털에 관리자 계정으로 로그인합니다. 포털의 검색창에서 "리소스 그룹"을 검색한 후 클릭합니다. [리소스 그룹] 블레이드에서 RG1lod<xxxxxxxx> 리소스 그룹을 클릭합니다.



2. [RG1lod<xxxxxxxx> 리소스 그룹] 블레이드의 [액세스 제어]로 이동합니다. 메뉴에서 [추가 - 역할 할당 추가]를 클릭합니다.



3. [역할 할당 추가] 블레이드의 [역할] 탭에서 "웹 사이트 참가자"를 검색한 후 선택하고 [다음]을 클릭합니다.



4. [구성원] 탭에서 "구성원 선택" 링크를 클릭합니다. [구성원 선택] 창에서 Dev-<xxxxxxxx> 계정을 검색한 후 선택하고 [선택]을 클릭합니다. [구성원] 탭에서 [검토 + 할당]을 클릭합니다. [검토 + 할당] 탭에서 [검토 + 할당]을 클릭합니다.

홈 > 리소스 그룹 > RG1lod33423492 | 액세스 제어(IAM) >

역할 할당 추가

역할 구성원 검토 + 할당

선택한 역할: 웹 사이트 참가자

다음에 대한 액세스 할당: ☒ 사용자, 그룹 또는 서비스 주체 ☐ 관리 ID

구성원: + 구성원 선택

이름	개체 ID	유형
선택한 구성원 없음		

Description: 선택 사항

구성원 선택

선택

사용자, 그룹 또는 서비스 보안 주체가 없습니다.

선택한 구성원:

DE Dev-33423492
 Dev-33423492@cloudslice.onmicrosoft.com 재거

- 동일한 방법으로 Dev-xxxxxxxx 계정에 다음과 같은 역할을 할당합니다.
 - 웹 플랜 참가자(Web Plan Contributor)
 - 네트워크 참가자(Network Contributor)
 - Storage 계정 참가자(Storage Account Contributor)
- [RG1lodxxxxxxxx] 리소스 그룹 블레이드의 [액세스 제어(IAM)]으로 이동합니다. [액세스 권한 확인] 탭에서 [액세스 권한 확인]을 클릭합니다. [액세스 확인] 창에서 Dev-xxxxxxxx 계정을 검색한 후 선택합니다.

홈 > 리소스 그룹 > RG1lod33423492

리소스 그룹

검색

개요 활동 로그 액세스 제어(IAM) 태그 리소스 시각화 도구 이벤트 설정 배포

액세스 권한 확인

내 액세스 이 리소스에 대한 내 액세스 수준 보기

내 액세스 보기

액세스 권한 확인 사용자, 그룹, 서비스 보안 주체 또는 관리 ID

액세스 권한 확인

액세스 확인

사용자, 그룹, 서비스 보안 주체 또는 관리 ID가 이 리소스에 대해 보유한 액세스 권한 수준을 검토하세요. [자세한 정보](#)

찾기

☒ 사용자, 그룹 또는 서비스 주체 ☐ 관리 ID

DE Dev-33423492
 Dev-33423492@cloudslice.onmicrosoft.com

- [Dev-xxxxxxxx] 할당 창에서 해당 계정이 "Storage 계정 참가자", "네트워크 참가자", "웹 사이트 참가자", "웹 플랜 참가자" 역할을 할당 받았는지 확인합니다.

홈 > 리소스 그룹 > RG1lod33423492

리소스 그룹

검색

개요 활동 로그 액세스 제어(IAM) 태그 리소스 시각화 도구 이벤트 설정 배포 보안 배포 스택 정책

Dev-33423492 할당 - RG1lod33423492

현재 역할 할당 적격 할당

이 범위에 상속되거나 이 범위에 있는 선택한 사용자, 그룹, 서비스 주체 또는 관리되는 ID에 대한 할당입니다.

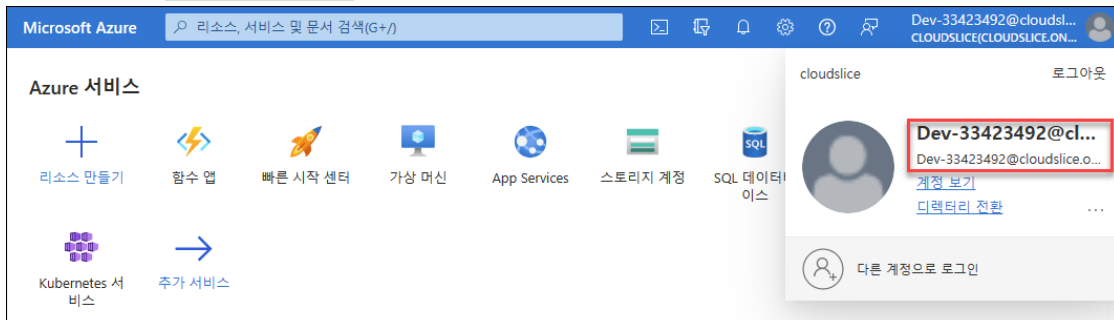
할당 이름이나 설명으로 검색

역할	설명	범위	그룹 할당	조건
LODReader	Lets you view everything, but no...	이 리소스	--	없음
Storage 계정 참가자	스토리지 계정 데이터에 대한 전...	이 리소스	--	없음
네트워크 참가자	네트워크를 관리할 수 있지만 역...	이 리소스	--	없음
웹 사이트 참가자	웹 사이트(웹 계획은 제외)를 관...	이 리소스	--	없음
웹 플랜 참가자	웹 사이트의 웹 계획을 관리할 수...	이 리소스	--	없음

거부 할당(0)

클래식 관리자(0)

8. Azure 포털에 Dev-**<xxxxxxxx>** 계정으로 로그인합니다.

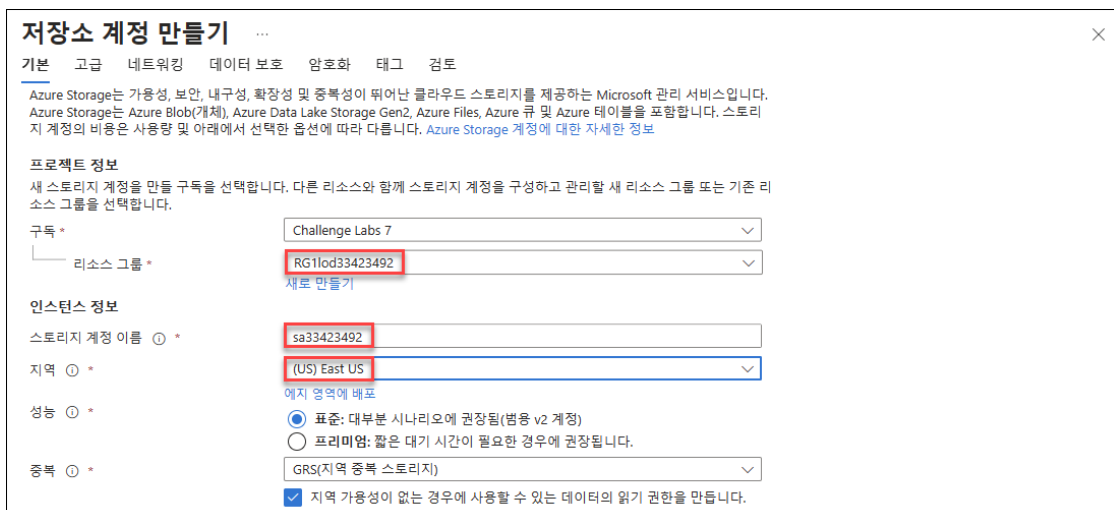


9. Azure 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다. [스토리지 계정] 블레이드에서 [만들기]를 클릭합니다.



10. [저장소 계정 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토]를 클릭합니다. [검토] 탭에서 [만들기]를 클릭합니다.

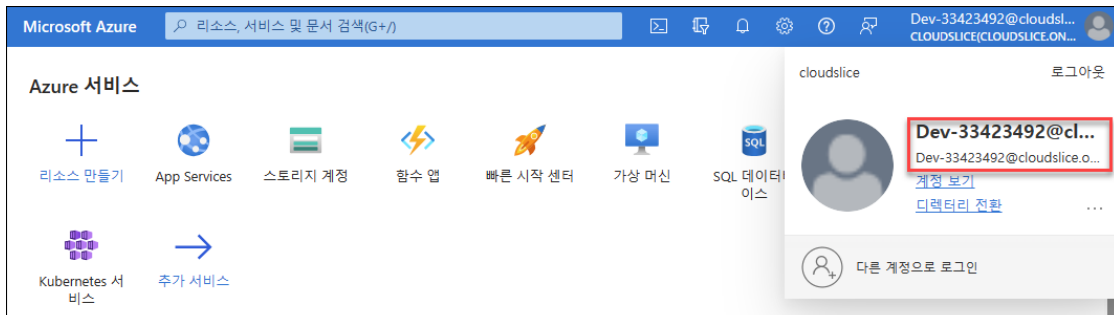
- [프로젝트 정보 - 리소스 그룹]: RG1lod**<xxxxxxxx>**
- [인스턴스 정보 - 스토리지 계정 이름]: sa**<xxxxxxxx>**
- [인스턴스 정보 - 지역]: (US) East US
- 다른 설정은 기본값을 사용합니다.



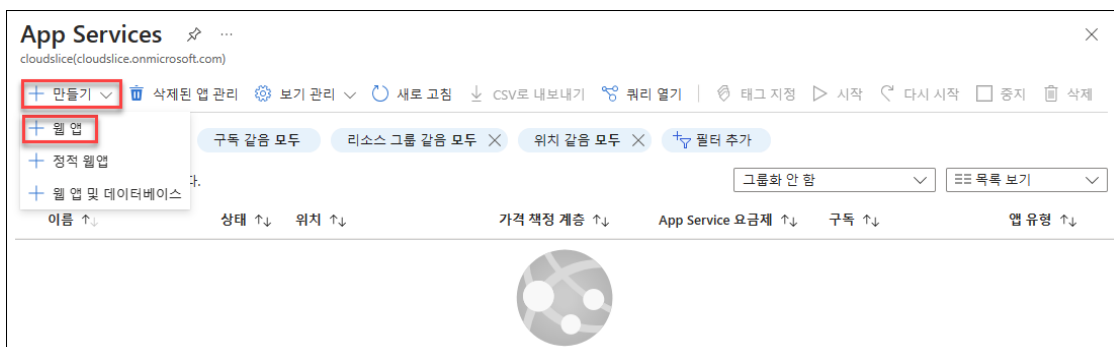
11. Dev-**<xxxxxxxx>** 계정에 스토리지 계정을 만들기 위한 역할이 할당되어 있기 때문에 스토리지 계정을 성공적으로 만들 수 있는 것을 확인합니다.

TASK 02. 개발자 계정으로 웹 앱 만들기

1. Azure 포털에 Dev-`<xxxxxxxx>` 계정으로 로그인합니다.



2. Azure 포털의 검색창에서 "App Services"를 검색한 후 클릭합니다. [App Services] 블레이드에서 [만들기 - 웹 앱]을 클릭합니다.



3. [웹앱 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

- [프로젝트 세부 정보 - 리소스 그룹]: RG1lod`<xxxxxxxx>`
- [인스턴스 정보 - 이름]: MyWebApp-`<xxxxxxxx>`
- [인스턴스 정보 - 게시]: 코드
- [인스턴스 정보 - 런타임 스택]: ASPNET V4.8
- [인스턴스 정보 - 운영 체제]: Windows
- [인스턴스 정보 - 지역]: East US
- [가격 책정 플랜 - Windows 플랜 (East US)]: "새로 만들기" 링크를 클릭한 후 "AppPlan1" 이름을 입력합니다.
- [가격 책정 플랜 - 가격 책정 플랜]: 표준 S1

웹앱 만들기 ...

기본 배포 네트워킹 모니터링 태그 검토 + 만들기

App Service Web Apps 사용하면 모든 플랫폼에서 실행되는 엔터프라이즈급 웹, 모바일 및 API 앱을 신속하게 구축, 배포 및 확장할 수 있습니다. 엄격한 성능, 확장, 보안 및 컴플라이언스 요구 사항을 충족하는 동시에 완전 관리형 플랫폼을 사용하여 인프라 유지 관리를 수행하세요. [자세히](#)

프로젝트 세부 정보
배포된 리소스와 비용을 관리할 구독을 선택합니다. 둘더 같은 리소스 그룹을 사용하여 모든 리소스를 정리 및 관리합니다.

구독 * ① Challenge Labs 7
리소스 그룹 * ① RG1lod33423492
[새로 만들기](#)

인스턴스 정보
데이터베이스가 필요한가요? 새 웹 + 데이터베이스 환경을 사용해 보세요. <3>

이름 * MyWebApp-33423492 .azurewebsites.net

게시 * ☒ 코드 ☐ Docker 컨테이너 ☐ 정적 웹 앱

런타임 스택 * ASP.NET V4.8

운영 체제 * ☐ Linux ☒ Windows

지역 * East US
App Service 플랜을 찾지 못하시겠습니까? 다른 지역을 시도하거나 App Service Environment를 선택하세요.

가격 책정 플랜
App Service 요금제 가격 책정 계층은 사용자 앱과 연관된 위치, 기능, 비용 및 컴퓨팅 리소스를 결정합니다. [자세히](#)

Windows 플랜 (East US) * ① (신규) AppPlan1
[새로 만들기](#)

가격 책정 플랜 표준 S1 (100 종 ACU, 1.75GB 메모리, 1 vCPU)
[가격 책정 플랜 살펴보기](#)

영역 중복
App Service 요금제는 이를 지원하는 지역에서 영역 중복 서비스로 배포될 수 있습니다. 이는 배포 시간만 결정하는 것입니다. 배포 후에는 App Service 요금제 영역 중복을 만들 수 없습니다. [자세히](#)

영역 중복
☐ 사용: App Service 요금제와 그 안의 앱은 영역 중복이 됩니다. 최소 App Service 계획 인스턴스 수는 3입니다.
☒ 사용 안 함: App Service 요금제와 그 안의 앱은 영역 중복이 아닙니다. 최소 App Service 계획 인스턴스 수는 1입니다.

4. 새로 만든 [MyWebApp-**<xxxxxxxx>**] 웹 앱] 블레이드로 이동합니다. [MyWebApp-**<xxxxxxxx>**] 웹 앱] 블레이드의 [배포 - 배포 센터]로 이동한 후 [FTPS credentials] 탭을 클릭합니다. [FTPS credentials] 탭의 "User scope"에서 다음 값을 입력한 후 메뉴에서 [Save]를 클릭합니다.

- Username: ftp<xxxxxxxx>
- Password: Pa55w.rd1234

MyWebApp-33423492 | 배포 센터 ☆ ...

웹 앱

검색 < Save Discard Browse Manage publish profile Sync Leave Feedback

배포

배포 슬롯

배포 센터

설정

구성

인증

Application Insights

ID

백업

사용자 지정 도메인

인증서

네트워킹

스케일 업(App Service 요금제)

스케일 아웃(App Service 요금제)

웹 작업

MySQL in App

서비스 커넥터

Settings Logs **FTPS credentials ***

App Service supports multiple technologies to access, publish and modify the content of your app. FTPS credentials can be scoped to the application or the user.

FTPS endpoint
ftps://waws-prod-blu-445.ftps.azurewebsites.windows.net/site/wwwroot

Application scope
Application scope credentials are auto-generated and provide access only to this specific app or deployment slot. These credentials can be used with FTPS, Local Git and WebDeploy. They cannot be configured manually, but can be reset anytime. [Learn more](#)

FTPS Username
MyWebApp-33423492\MyWebApp-33423492

Password
..... Reset

User scope
User scope credentials are defined by you, the user, and can be used with all the apps to which you have access. These credentials can be used with FTPS, Local Git and WebDeploy. Authenticating to an FTPS endpoint using user-level credentials requires a username in the following format: 'MyWebApp-33423492\<your username>'. Authenticating with Git requires only the username '<your username>' defined below. [Learn more](#)

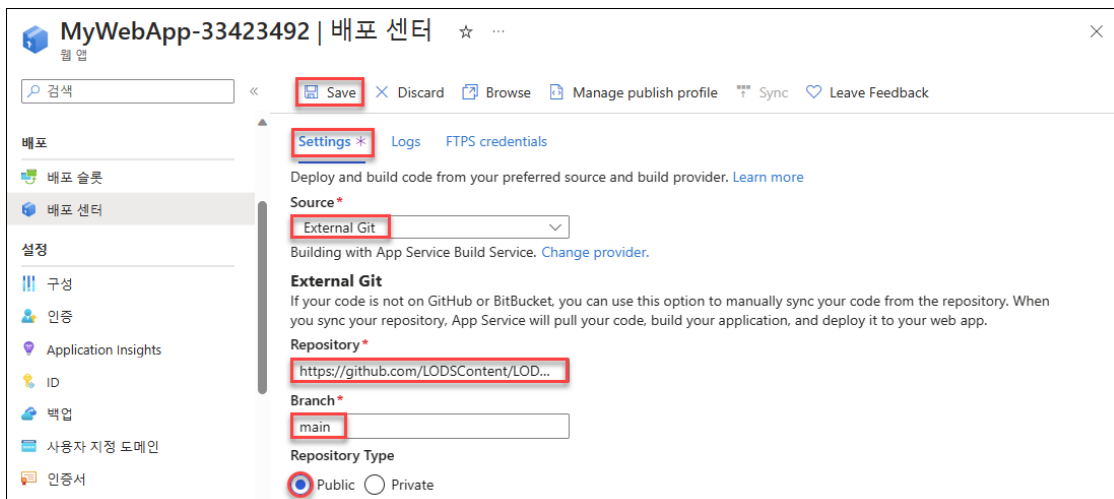
Username
ftp33423492

Password
..... Reset

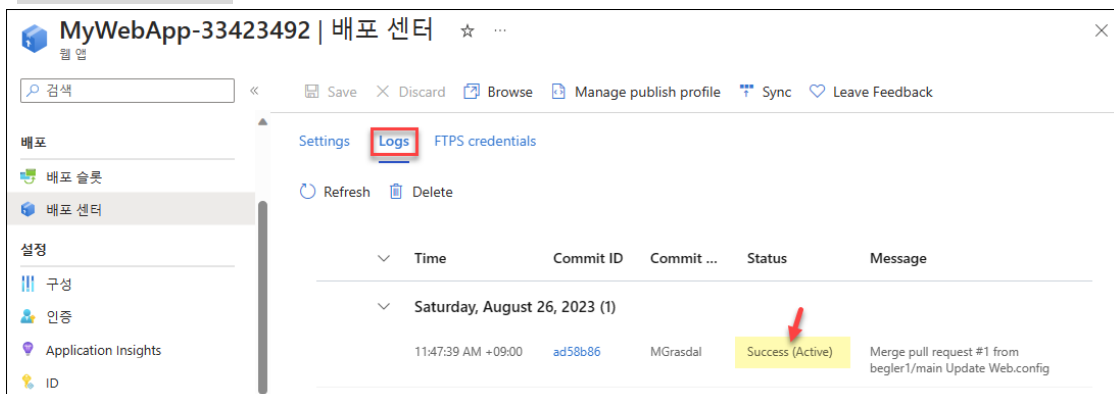
Confirm Password
.....

5. [MyWebApp-<xxxxxxxx>] 웹 앱 | 배포 센터] 블레이드에서 [Settings] 탭으로 이동한 후 아래와 같이 구성하고 [Save]를 클릭합니다.

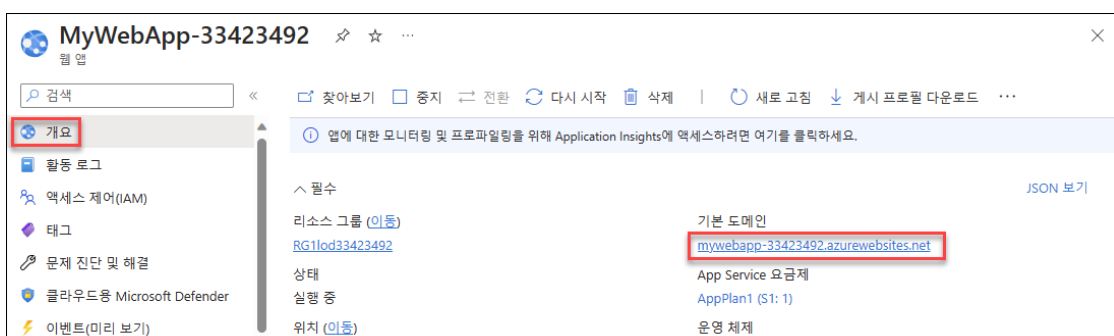
- Source: External Git
- [External Git - Repository]: https://github.com/L0DSContent/L0DS0C_app-service-web-dotnet-get-started
- [External Git - Branch]: main
- [External Git - Repository Type]: Public



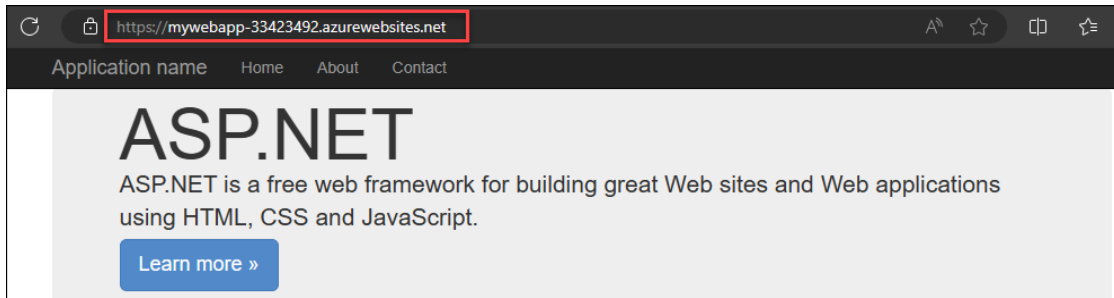
6. [MyWebApp-<xxxxxxxx>] 웹 앱 | 배포 센터] 블레이드에서 [Logs] 탭으로 이동한 후 배포 상태가 "Success (Active)"로 표시될 때까지 기다립니다.



7. [MyWebApp-<xxxxxxxx>] 웹 앱] 블레이드의 [개요]로 이동한 후 기본 도메인에 표시되는 링크를 클릭합니다.

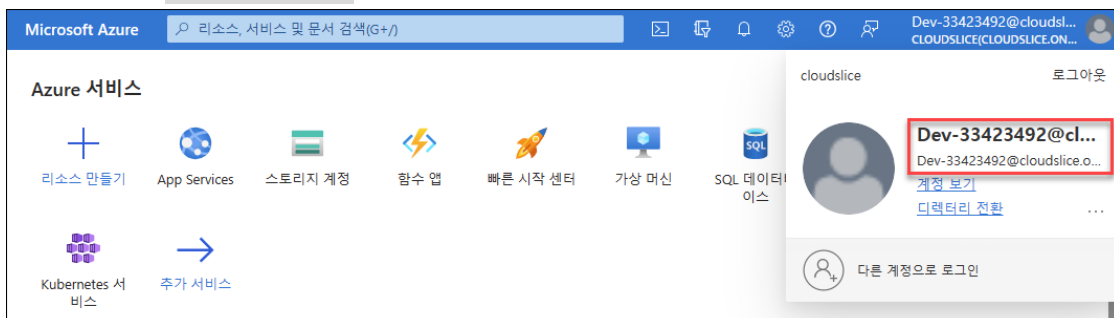


8. 아래와 같이 Git Repository에서 배포한 웹 사이트가 표시되는 것을 확인합니다.



TASK 03. 웹 앱과 가상 네트워크 통합

1. Azure 포털에 Dev-`<xxxxxxxx>` 계정으로 로그인합니다.



2. Azure 포털의 검색창에서 "가상 네트워크"를 검색한 후 클릭합니다. [가상 네트워크] 블레이드의 메뉴에서 [만들기]를 클릭합니다.



3. [가상 네트워크 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
 - [프로젝트 정보 - 리소스 그룹]: RG1lod<xxxxxxxx>
 - [인스턴스 정보 - 가상 네트워크 이름]: VNET-<xxxxxxxx>
 - [인스턴스 정보 - 지역]: (US) East US

가상 네트워크 만들기 ...

기본 사항 보안 IP 주소 태그 검토 + 만들기

VNet(Azure Virtual Network)은 Azure에서 프라이빗 네트워크의 기본 빌딩 블록입니다. VNet을 사용하면 Azure Virtual Machines(VM)과 같은 다양한 유형의 Azure 리소스가 서로 통신하거나 인터넷 및 온-프레미스 네트워크와 안전하게 통신할 수 있습니다. VNet은 데이터 센터에서 작동하는 전통적인 네트워크와 유사하지만, 확장, 가용성, 격리 등 Azure 인프라의 추가 혜택을 제공합니다.

[자세한 정보](#)

프로젝트 정보
 배포된 리소스 및 비용을 관리할 구독을 선택합니다. 폴더와 같은 리소스 그룹을 사용하여 모든 리소스를 구성하고 관리합니다.

구독 * Challenge Labs 7

리소스 그룹 * RG1od33423492
[새로 만들기](#)

인스턴스 정보
 가상 네트워크 이름 * VNET-33423492

지역 ① * (US) East US
[여기 영역에 배포](#)

4. [MyWebApp-<xxxxxxxx>] 웹 앱] 블레이드의 [설정 - 네트워킹]으로 이동합니다. [아웃바운드 트래픽] 타일의 "VNet 통합" 링크를 클릭합니다.

MyWebApp-33423492 | 네트워킹 ☆ ...

웹 앱

검색 << 새로 고침 네트워크 문제 해결사 피드백 보내기

설정

- 구성
- 인증
- Application Insights
- ID
- 백업
- 사용자 지정 도메인
- 인증서
- 네트워킹**
- 스케일 업(App Service 요금제)
- 스케일 아웃(App Service 요금제)
- 웹 작업

웹앱의 네트워킹 구성을 확인하세요. 나열된 기능 중 하나를 선택하여 네트워킹 설정을 변경하세요. [자세한 정보](#)

인바운드 트래픽	웹앱	아웃바운드 트래픽
역세스 및 들어오는 서비스를 관리합니다.	해당 사용자 지정 도메인은 웹앱에 트래픽을 전송합니다.	데이터베이스와 같은 앱 종속성에 대한 호출을 설정합니다.
기능 액세스 제한 <input type="radio"/> 끄기 앱 할당 주소 <input type="radio"/> 끄기 프라이빗 엔드포인트 <input type="radio"/> 끄기	도메인 mywebapp-33423492.azurewebsites.net	기능 VNet 통합 <input type="radio"/> 끄기 하이브리드 연결 <input type="radio"/> 끄기
인바운드 주소 20.119.0.35		아웃바운드 주소 ① 20.119.104.105, 20.85.198.153, 20.119.108.191, 20.119.109.110 ...자세히 표시

5. [VNet 통합] 블레이드에서 [VNet 추가]를 클릭합니다. [VNet 통합 추가] 창에서 아래와 같이 구성한 후 [확인]을 클릭합니다.

- Virtual Network: VNET-<xxxxxxxx> (East US)
- 서브넷: 기존 항목 선택
- 서브넷: default (10.0.0.0 - 10.0.0.255)

VNet 통합 ...

mywebapp-33423492

[연결 끊기](#) [새로 고침](#) [문제 해결](#)

VNet 구성

Azure VNet에서 또는 Azure VNet을 통해 사용할 수 있는 리소스에 안전하게 액세스

+ VNet 추가

VNet 세부 정보

VNet 이름 구성되지 않음
 위치 구성되지 않음

VNet 통합 추가

mywebapp-33423492

클래식 VNet에 연결하려면 여기를 클릭하세요. →

구독 Challenge Labs 7

Virtual Network VNET-33423492 (East US)

서브넷
☐ 새 서브넷 만들기 ☒ 기존 항목 선택

서브넷 default (10.0.0.0 - 10.0.0.255)