한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. Challenge Lab 09

LAB 05. AKS를 사용하여 보안 구성

Microsoft

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

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.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2023.08.31	1.0.0	우진환	LAB 05 내용 작성

목차

도전 과제

이 실습에서는 AKS (Azure Kubernetes Service)를 사용하여 안전한 컨테이너화된 애플리케이션을 배포합니다.

- AKS 클러스터를 만들고 클러스터에 RBAC 역할을 할당합니다.
- Azure Cloud Shell을 사용하여 관리자로 AKS 클러스터에 연결합니다.
- AKS 클러스터에 개발자로 애플리케이션을 배포한 다음 클러스터 보안을 확인합니다.

STEP 01. AKS 클러스터 배포

1. 다음 속성을 사용하여 AKS 클러스터를 배포합니다.

속성	값
리소스 그룹	corp-datalod<XXXXXXXXX>
클러스터 사전 설정 구성	표준
Kubernetes 클러스터 이름	aks
가용성 영역	없음
노드 크기	Standard DS2_v2 - 2 vcpu, 8 GiB 메모리
노드 수	최대 2 개
인증 및 권한 부여	Kubernetes RBAC 가 있는 로컬 계정
컨테이너 모니터링	모두 사용하지 않습니다.

2. 새로 만든 Kubernetes 서비스에서 액세스 제어를 구성합니다. `User1-<XXXXXXXX>` 계정이 "`Azure Kubernetes Service 클러스터 사용자 역할`"을 가지도록 설정합니다.

STEP 02. 관리자로 AKS 클러스터 연결

1. Cloud Shell의 Bash 세션을 다음 정보를 사용하여 시작합니다.

속성	값
리소스 그룹	corp-datalod<XXXXXXXXX>
Cloud Shell 지역	미국 동부
스토리지 계정	cs<XXXXXXXXX>
파일 공유	cloudshell

2. Cloud Shell에서 `az aks get-credentials` 명령을 실행하여 AKS 클러스터에 연결합니다.
3. Cloud Shell에서 `kubectl config current-context` 명령을 실행하여 컨텍스트를 확인합니다.
4. Cloud Shell에서 `kubectl get` 명령을 실행하여 노드를 확인합니다.

STEP 03. Non-administrative 사용자로 AKS 클러스터에 컨테이너 배포

1. `User1-<XXXXXXXX>` 계정으로 포털에 로그인한 후 다음 정보를 사용하여 Cloud Shell의 Bash 세션을 시작합니다.

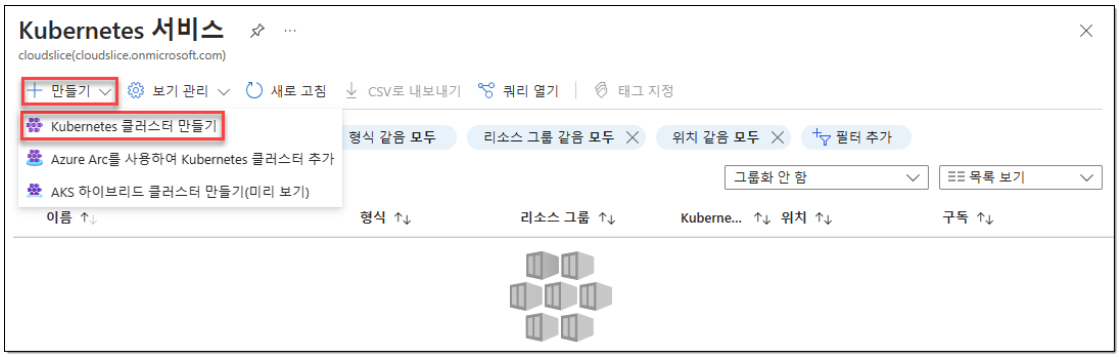
속성	값
리소스 그룹	corp-datalod<XXXXXXXXX>
Cloud Shell 지역	미국 동부
스토리지 계정	cs<XXXXXXXXX>

파일 공유	cloudshell

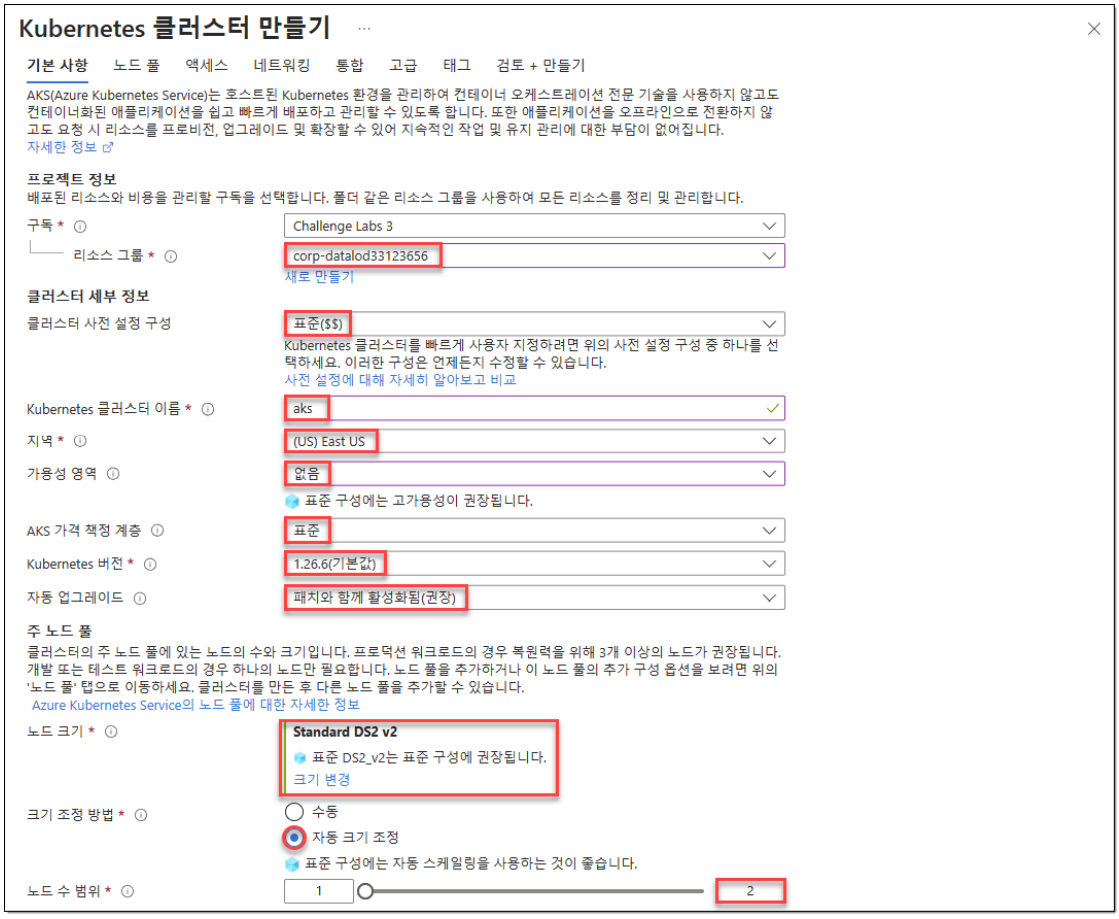
2. Cloud Shell에서 `az aks get-credentials` 명령을 사용하여 AKS 클러스터에 연결합니다.
3. Cloud Shell에서 `kubectl config` 명령을 실행하여 현재 컨텍스트를 확인합니다.
4. Cloud Shell에서 `az aks stop` 명령을 실행하여 AKS 클러스터를 중지합니다. 권한 부족으로 인해 명령이 실패하는 것을 확인합니다.
5. Cloud Shell에서 `kubectl create deployment` 명령을 실행하여 nginx 이미지를 사용하는 컨테이너를 만듭니다.
6. Cloud Shell에서 `kubectl get` 명령을 실행하여 배포한 `Pod`를 확인합니다.
7. Cloud Shell에서 `kubectl expose deployment` 명령을 실행하여 새 `Service` 개체를 만듭니다.
8. Cloud Shell에서 `kubectl get services` 명령을 실행하여 공용 IP를 확인한 후 연결을 확인합니다.

TASK 01. RBAC을 사용하는 AKS 클러스터 배포

1. Azure 포털의 검색창에서 "`Kubernetes 클러스터`"를 검색한 후 클릭합니다. [Kubernetes 서비스] 블레이드에서 [만들기 - Kubernetes 클러스터 만들기]를 클릭합니다.



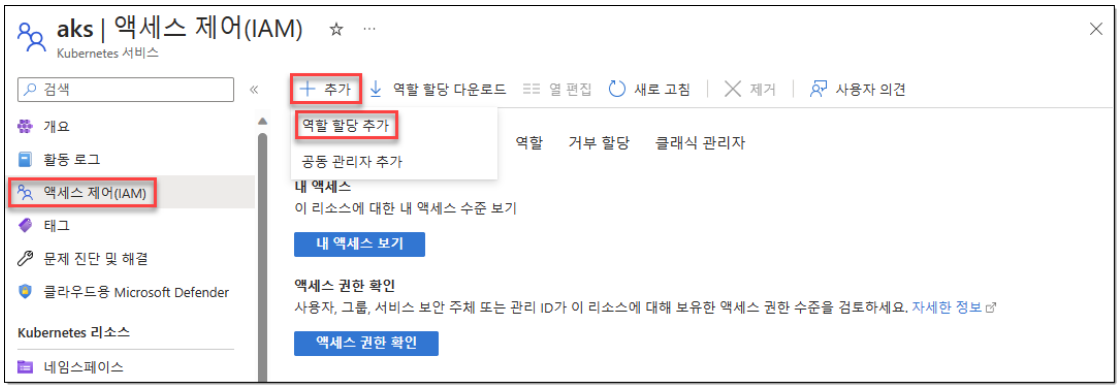
2. [Kubernetes 클러스터 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [액세스] 탭으로 이동합니다.
   - [프로젝트 정보 - 리소스 그룹]: `corp-datalod<XXXXXXXX>`
   - [클러스터 세부 정보 - 클러스터 사전 설정 구성]: 표준($$)
   - [클러스터 세부 정보 - Kubernetes 클러스터 이름]: aks
   - [클러스터 세부 정보 - 지역]: (US) East US
   - [클러스터 세부 정보 - 가용성 영역]: 없음
   - [클러스터 세부 정보 - AKS 가격 책정 계층]: 표준
   - [클러스터 세부 정보 - Kubernetes 버전]: 기본값 버전을 사용합니다.
   - [클러스터 세부 정보 - 자동 업그레이드]: 패치와 함께 활성화됨
   - [주 노드 풀 - 노드 크기]: Standard DS2 v2
   - [주 노드 풀 - 크기 조정 방법]: 자동 크기 조정
   - [주 노드 풀 - 노드 수 범위]: 최대 2대로 설정합니다.



3. [액세스] 탭에서 인증 및 권한 부여를 "Kubernetes RBAC가 있는 로컬 계정"으로 선택한 후 [통합] 탭으로 이동합니다.

4. [통합] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - 컨테이너 인사이트: 선택하지 않습니다.
   - 관리되는 Prometheus: 선택하지 않습니다.
   - 관리 Grafana: 선택하지 않습니다.
   - 경고 중: 선택하지 않습니다.
   - Azure Policy: 사용 안 함

5. [aks Kubernetes 서비스] 블레이드의 [액세스 제어]로 이동한 후 메뉴에서 [추가 - 역할 할당 추가]를 클릭합니다.

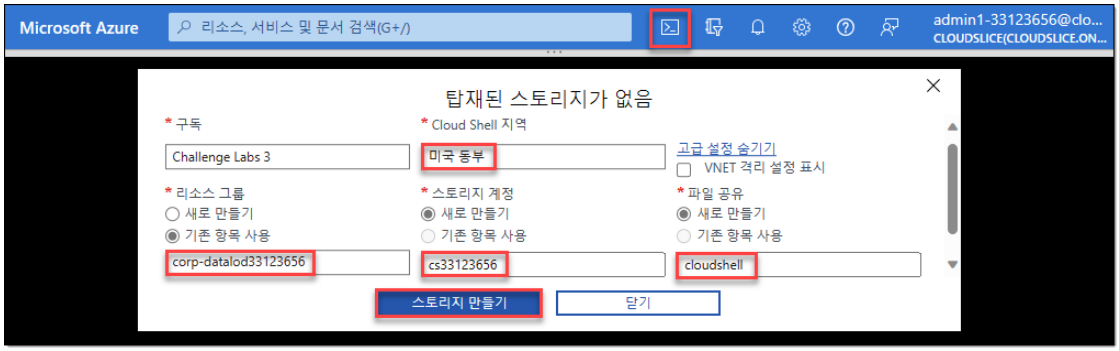


6. [역할 할당 추가] 블레이드의 [역할]에서 "Kubernetes"로 검색한 후 "Azure Kubernetes Service 클러스터 사용자 역할"을 선택하고 [다음]을 클릭합니다.

7. [구성원] 탭에서 "구성원 선택"을 클릭합니다. [구성원 선택] 창에서 "User1-<XXXXXXXXX>"을 검색한 후 선택하고 [선택]을 클릭합니다. [구성원] 탭에서 [검토 + 할당]을 클릭합니다. [검토 + 할당] 탭에서 [검토 + 할당]을 클릭합니다.

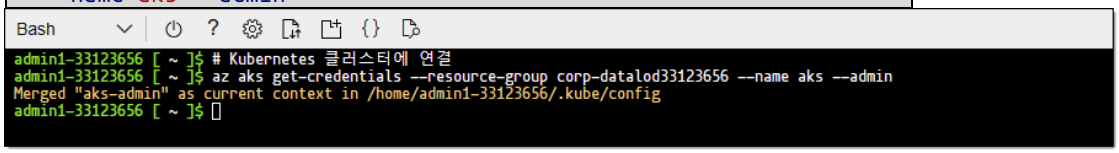
TASK 02. 관리자로 AKS 클러스터에 연결

1. Azure 포털의 우측 상단에서 [Cloud Shell] 아이콘을 클릭한 후 "Bash"를 선택합니다. [탑재된 스토리지가 없음] 창에서 "고급 설정 표시"를 클릭합니다. [탑재된 스토리지가 없음] 페이지에서 아래와 같이 구성한 후 [스토리지 만들기]를 클릭합니다.
   - Cloud Shell 지역: 미국 동부
   - 리소스 그룹: corp-datalod<XXXXXXXX>
   - 스토리지 계정: cs<XXXXXXXX>
   - 파일 공유: cloudshell



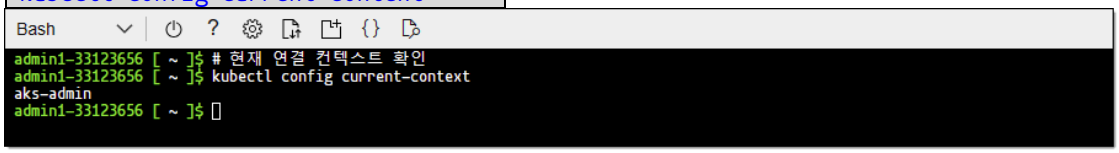
2. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 AKS 클러스터에 연결합니다.

```
# Kubernetes 클러스터에 연결
az aks get-credentials --resource-group corp-datalod<XXXXXXXX> \
  --name aks --admin
```



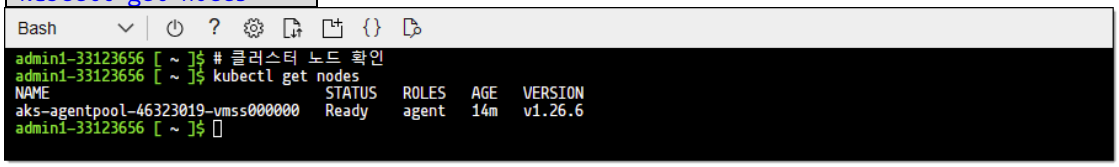
3. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 클러스터 연결에 대한 현재 컨텍스트를 확인합니다. 명령 출력에서 현재 컨텍스트가 "`aks-admin`"으로 표시되는지 확인합니다.

```
# 현재 연결 컨텍스트 확인
kubectl config current-context
```



4. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 클러스터 노드 목록을 확인합니다.

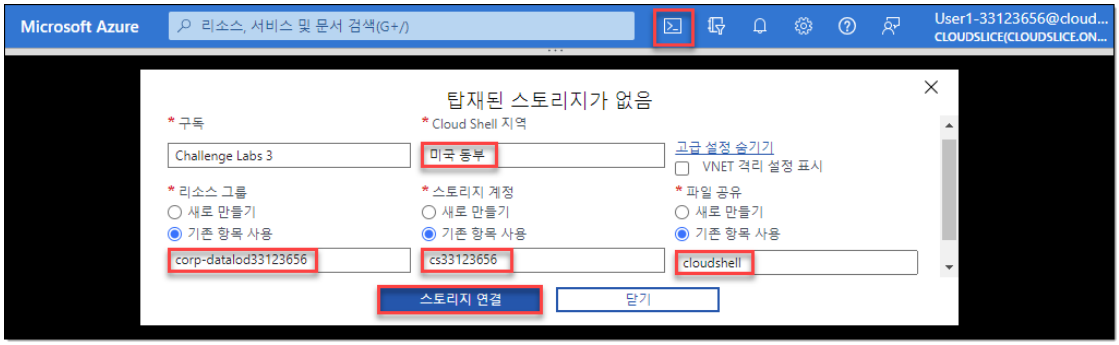
```
# 클러스터 노드 확인
kubectl get nodes
```



TASK 03. non-administrative 사용자로 AKS 클러스터에 컨테이너 배포

1. Microsoft Edge 브라우저에서 InPrivate 창을 열고 Azure 포털에 연결합니다. 개발자 계정(`User1-<XXXXXXXX>`)을 사용하여 로그인합니다.
2. Azure 포털의 우측 상단에서 [Cloud Shell] 아이콘을 클릭한 후 "`Bash`"를 선택합니다. [탑재된 스토리지가 없음] 창에서 "`고급 설정 표시`"를 클릭합니다. [탑재된 스토리지가 없음] 페이지에서 아래와 같이 구성한 후 [스토리지 연결]을 클릭합니다. 로그인 사용자 계정은 Azure 포털에 읽기 액세스 권한만 있기 때문에 파일 공유 탑재와 관련된 오류가 발생하며 이는 무시할 수 있습니다.
   - Cloud Shell 지역: 미국 동부
   - 리소스 그룹: `corp-datalod<XXXXXXXX>`

- 스토리지 계정: "기존 항목 사용"을 선택한 후 "cs<XXXXXXXXX>" 계정을 선택합니다.
- 파일 공유: "기존 항목 사용"을 선택한 후 "cloudshell"을 입력합니다.



3. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 사용자 컨텍스트로 Kubernetes 클러스터에 연결합니다.

```
# Kubernetes에 사용자 컨텍스트로 연결
az aks get-credentials --resource-group corp-datalod<XXXXXXXXX> --name aks
```

```
Bash
user1-33123656 [ ~ ]$ # Kubernetes에 사용자 컨텍스트로 연결
user1-33123656 [ ~ ]$ az aks get-credentials --resource-group corp-datalod33123656 --name aks
Merged "aks" as current context in /home/user1-33123656/.kube/config
user1-33123656 [ ~ ]$
```

4. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 클러스터에 연결된 현재 컨텍스트를 확인합니다. 컨텍스트가 "aks"로 표시되는 것을 확인합니다.

```
# 현재 연결 컨텍스트 확인
kubectl config current-context
```

```
Bash
user1-33123656 [ ~ ]$ # 현재 연결 컨텍스트 확인
user1-33123656 [ ~ ]$ kubectl config current-context
aks
user1-33123656 [ ~ ]$
```

5. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 Kubernetes 클러스터를 중지합니다. 현재 컨텍스트에서 클러스터에 대한 권한이 없기 때문에 아래와 같이 오류가 발생하는 것을 확인할 수 있습니다.

```
# AKS 클러스터 중지
az aks stop --resource-group corp-datalod<XXXXXXXXX> --name aks
```

```
Bash
user1-33123656 [ ~ ]$ # AKS 클러스터 중지
user1-33123656 [ ~ ]$ az aks stop --resource-group corp-datalod33123656 --name aks
(AuthorizationFailed) The client 'User1-33123656@cloudslice.onmicrosoft.com' with object id 'c280331e-0272-4bc3-8c15-da9343e72c5
ion to perform action 'Microsoft.ContainerService/managedClusters/stop/action' over scope '/subscriptions/4a5a6077-91a6-4b7a-ae
ps/corp-datalod33123656/providers/Microsoft.ContainerService/managedClusters/aks' or the scope is invalid. If access was recentl
our credentials.
Code: AuthorizationFailed
Message: The client 'User1-33123656@cloudslice.onmicrosoft.com' with object id 'c280331e-0272-4bc3-8c15-da9343e72c5d' does not h
m action 'Microsoft.ContainerService/managedClusters/stop/action' over scope '/subscriptions/4a5a6077-91a6-4b7a-ae62-a2ed402b1a7
od33123656/providers/Microsoft.ContainerService/managedClusters/aks' or the scope is invalid. If access was recently granted, pl
ls.
user1-33123656 [ ~ ]$
```

6. [Cloud Shell]의 Bash 세션에서 nginx 이미지를 사용하는 Deployment를 배포합니다.

```
# nginx 이미지로 새 Deployment 배포
kubectl create deployment nginx-<XXXXXXXXX> --image=nginx
```

```
Bash
user1-33123656 [ ~ ]$ # nginx 이미지로 새 Deployment 배포
user1-33123656 [ ~ ]$ kubectl create deployment nginx-33123656 --image=nginx
deployment.apps/nginx-33123656 created
user1-33123656 [ ~ ]$
```

7. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 애플리케이션에 대한 `Pod`가 생성되었는지 확인합니다.

```
# 배포한 Pod 확인
kubectl get pods
```

```
Bash
user1-33123656 [ ~ ]$ # 배포한 Pod 확인
user1-33123656 [ ~ ]$ kubectl get pods
NAME                              READY   STATUS    RESTARTS   AGE
nginx-33123656-b76b9897f-x64z9   1/1     Running   0          69s
user1-33123656 [ ~ ]$
```

8. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 `Service` 개체를 만들어 `Pod`를 인터넷에 노출시킵니다.

```
# Service 개체 배포
kubectl expose deployment nginx-<XXXXXXXXX> --port=80 --type=LoadBalancer
```

```
Bash
user1-33123656 [ ~ ]$ # Service 개체 배포
user1-33123656 [ ~ ]$ kubectl expose deployment nginx-33123656 --port=80 --type=LoadBalancer
service/nginx-33123656 exposed
user1-33123656 [ ~ ]$
```

9. [Cloud Shell]의 Bash 세션에서 다음 명령을 실행하여 `Service` 개체에 할당된 공용 IP 주소를 확인합니다. `EXTERNAL-IP` 열의 값이 공용 IP이며 이 IP 주소를 메모장에 복사합니다.

```
# 배포한 Service 확인
kubectl get services
```

```
Bash
user1-33123656 [ ~ ]$ # 배포한 Service 확인
user1-33123656 [ ~ ]$ kubectl get services
NAME              TYPE           CLUSTER-IP    EXTERNAL-IP    PORT(S)        AGE
kubernetes        ClusterIP      10.0.0.1      <none>         443/TCP        29m
nginx-33123656    LoadBalancer   10.0.222.92   20.81.35.207   80:31324/TCP   41s
user1-33123656 [ ~ ]$
```

10. 브라우저에서 새 탭을 열고 위에서 복사한 공용 IP 주소에 액세스합니다. 아래와 같이 NGINX 웹 페이지가 표시되는 것을 확인합니다.