

한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. LAB11

모니터링 구현

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
2021.11.25	1.0.0	우진환	LAB11 작성
2022.10.08	1.1.0	우진환	Azure 포털 변경 사항 적용
2023.02.12	1.2.0	우진환	Cloudslice 변경 사항 적용
2023.06.04	1.3.0	우진환	Cloudslice 변경 사항 적용

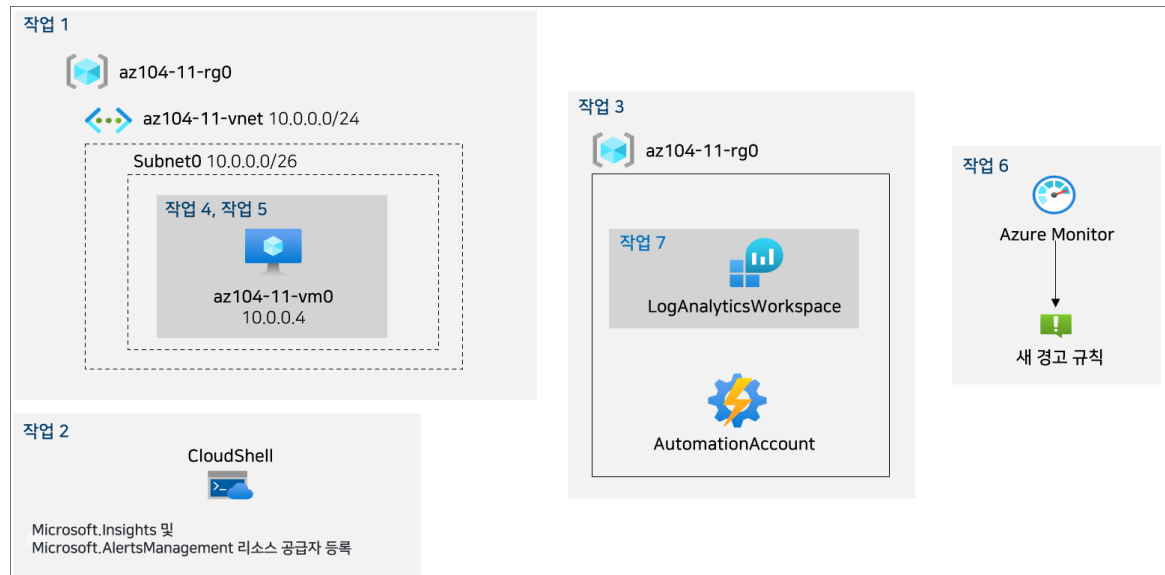
목차

실습 시나리오	4
아키텍처 다이어그램	4
TASK 01. 실습 환경 프로비저닝	4
TASK 02. MICROSOFT.INSIGHTS와 MICROSOFT.ALERTSMANAGEMENT 리소스 공급자 등록.....	6
TASK 03. AZURE LOG ANALYTICS 작업 영역과 AZURE AUTOMATION 기반 솔루션 생성 및 구성.....	6
TASK 04. AZURE 가상 머신의 기본 모니터링 설정 검토.....	10
TASK 05. AZURE 가상 머신 진단 설정 구성	11
TASK 06. AZURE MONITOR 기능 검토	14
TASK 07. AZURE LOG ANALYTICS 기능 검토	19
TASK 08. 리소스 정리	22

실습 시나리오

Azure 가상 머신에 중점을 두고 Azure 리소스의 성능 및 구성에 대한 인사이트를 제공하는 Azure 기능을 평가해야 합니다. 이를 위해 Log Analytics를 비롯한 Azure Monitor의 기능을 검사하려 합니다.

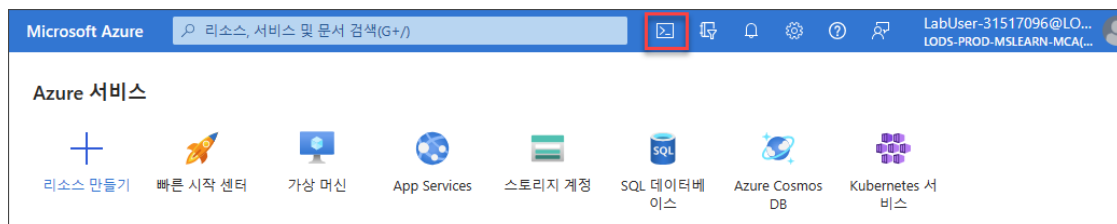
아키텍처 다이어그램



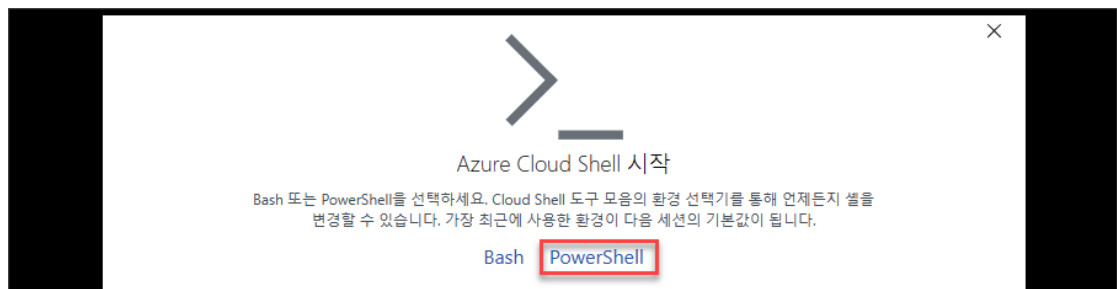
TASK 01. 실습 환경 프로비저닝

이 작업에서는 모니터링 시나리오를 테스트하는데 사용할 가상 머신을 배포합니다.

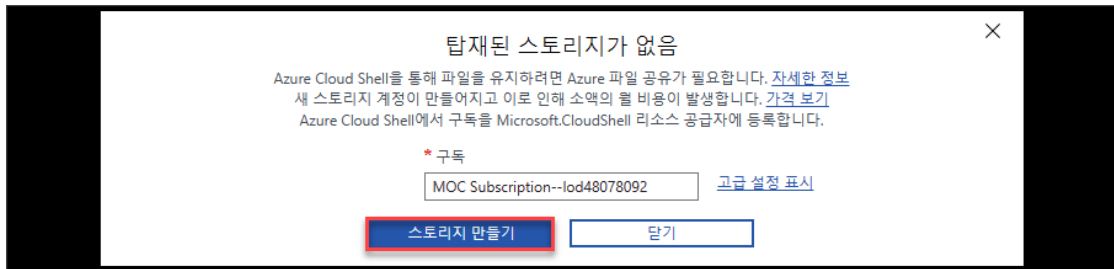
1. Azure 포털의 우측 상단에서 [Cloud Shell] 아이콘을 클릭합니다.



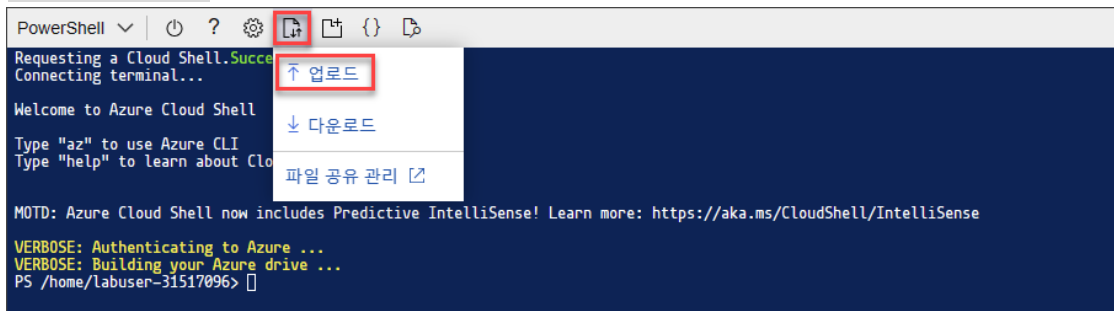
2. [Azure Cloud Shell 시작] 창에서 [PowerShell]을 클릭합니다.



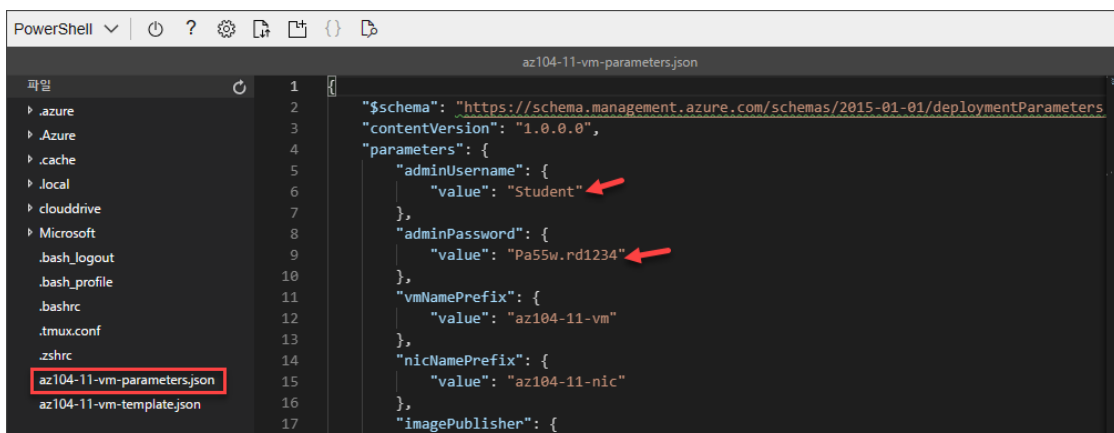
3. [탐재된 스토리지가 없음] 페이지에서 [스토리지 만들기]를 클릭합니다.



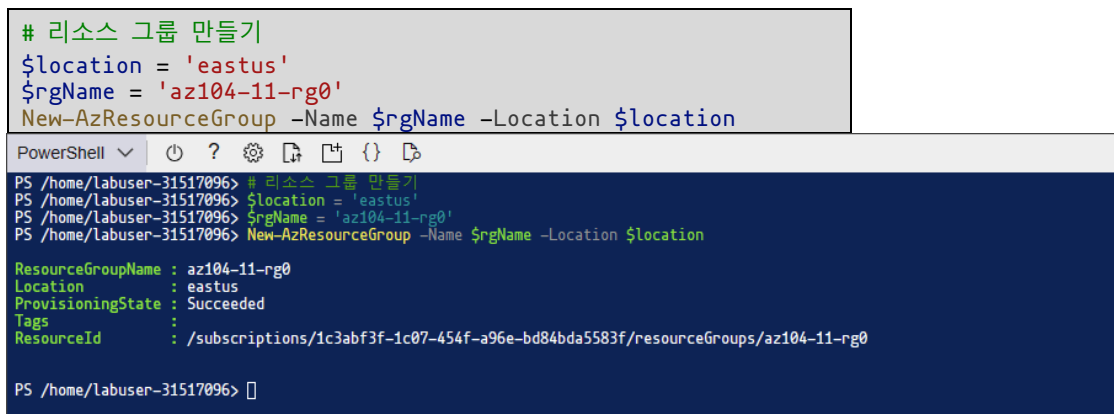
4. Azure 포털에서 [Cloud Shell]을 엽니다. PowerShell 세션에서 [파일 업로드/다운로드 - 업로드]를 클릭한 후 "Labs\11\az104-11-vm-template.json" 파일과 "Labs\11\az104-11-vm-parameters.json" 파일을 업로드합니다.



5. 실습에서 가상 머신 로그인에 사용되는 사용자 계정과 암호를 변경하고자 하는 경우 [Cloud Shell]에서 [편집기 열기]를 클릭한 후 az104-11-vm-parameters.json 파일을 열고 계정과 암호를 변경할 수 있습니다.



6. [Cloud Shell]에서 다음 명령을 실행하여 가상 머신을 호스팅할 리소스 그룹을 생성합니다.



7. [Cloud Shell]에서 다음 명령을 실행하여 업로드한 템플릿 파일과 매개 변수 파일을 사용하여 가상 네트워크를 만들고 이 가상 네트워크에 가상 머신을 배포합니다.

```
# 템플릿을 사용하여 가상 네트워크와 가상 머신 만들기
New-AzResourceGroupDeployment `
  -ResourceGroupName $rgName `
  -TemplateFile $HOME/az104-11-vm-template.json `
  -TemplateParameterFile $HOME/az104-11-vm-parameters.json `
  -AsJob
```

PowerShell

```
PS /home/labuser-31517096> # 템플릿을 사용하여 가상 네트워크와 가상 머신 만들기
PS /home/labuser-31517096> New-AzResourceGroupDeployment `
>> -ResourceGroupName $rgName `
>> -TemplateFile $HOME/az104-11-vm-template.json `
>> -TemplateParameterFile $HOME/az104-11-vm-parameters.json `
>> -AsJob
```

Id	Name	PSJobTypeName	State	HasMoreData	Location	Command
2	Long Running 0	AzureLongRunni	Running	True	localhost	New-AzResourceGroupDeplo...

```
PS /home/labuser-31517096> []
```

TASK 02. Microsoft.Insights와 Microsoft.AlertsManagement 리소스 공급자 등록

1. [Cloud Shell]에서 다음 명령을 실행하여 Microsoft.Insights와 Microsoft.AlertsManagement 리소스 공급자를 등록합니다.

```
# 리소스 공급자 등록
Register-AzResourceProvider -ProviderNamespace Microsoft.Insights
Register-AzResourceProvider -ProviderNamespace Microsoft.AlertsManagement
```

PowerShell

```
PS /home/labuser-31517096> # 리소스 공급자 등록
PS /home/labuser-31517096> Register-AzResourceProvider -ProviderNamespace Microsoft.Insights
```

```
ProviderNamespace : microsoft.insights
RegistrationState  : Registering
ResourceTypes     : {components, components/query, components/metadata, components/metrics_}
Locations         : {East US, South Central US, North Europe, West Europe_}
```

```
PS /home/labuser-31517096> Register-AzResourceProvider -ProviderNamespace Microsoft.AlertsManagement
```

```
ProviderNamespace : Microsoft.AlertsManagement
RegistrationState  : Registered
ResourceTypes     : {alerts, alertsSummary, smartGroups, smartDetectorAlertRules_}
Locations         : {global, North Central US, West Central US, East US_}
```

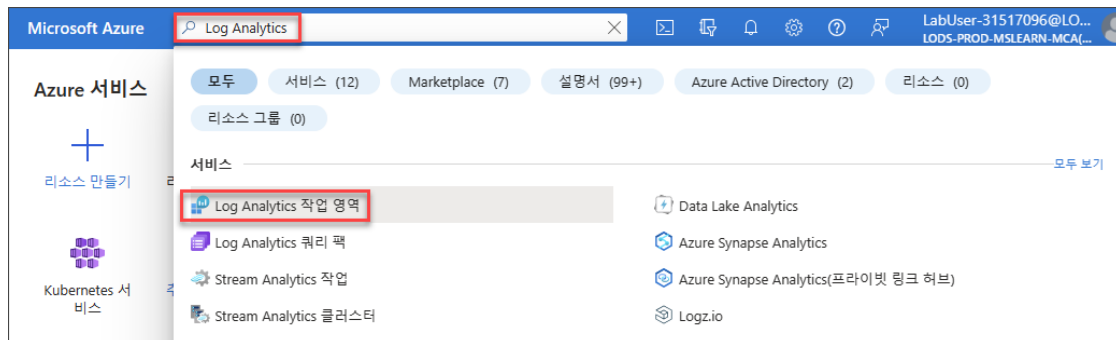
```
PS /home/labuser-31517096> []
```

2. [Cloud Shell]을 최소화합니다.

TASK 03. Azure Log Analytics 작업 영역과 Azure Automation 기반 솔루션 생성 및 구성

이 작업에서는 Azure Log Analytics 작업 영역과 Azure Automation 기반 솔루션을 만들고 구성합니다.

1. Azure 포털의 검색창에서 "Log Analytics"를 검색한 후 [Log Analytics 작업 영역]을 클릭합니다.

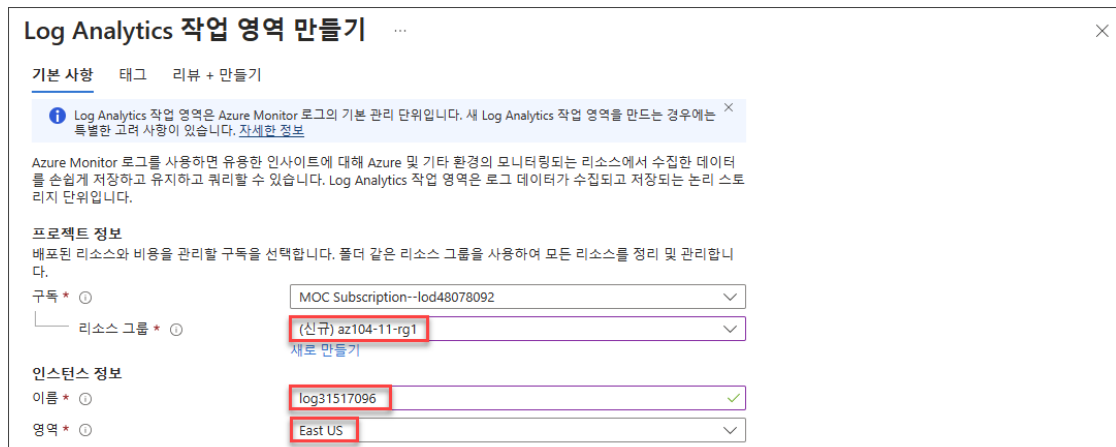


2. [Log Analytics 작업 영역] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

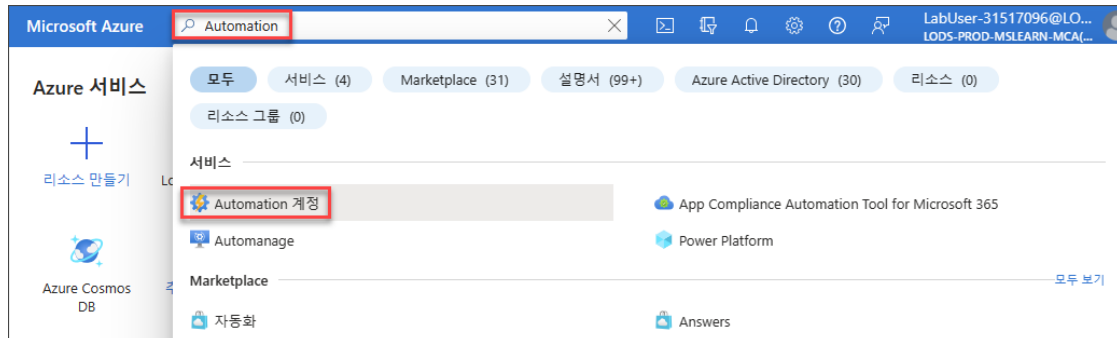


3. [Log Analytics 작업 영역 만들기] 블레이드의 [기본 사항] 탭에서 다음과 같이 구성하고 [리뷰 + 만들기]를 클릭합니다. [리뷰 + 만들기] 탭에서 [만들기]를 클릭합니다.

- [프로젝트 정보 - 리소스 그룹]: "새로 만들기"를 클릭한 후 "az104-11-rg1"을 입력합니다.
- [인스턴스 정보 - 이름]: log<xxxxxxxx> 이름을 입력합니다. <xxxxxxxx>은 구독 계정 뒤의 숫자를 입력합니다.
- [인스턴스 정보 - 영역]: East US



4. Azure 포털의 검색창에서 "automation"을 검색한 후 [Automation 계정]을 클릭합니다.



5. [Automation 계정] 블레이드의 메뉴에서 [만들기]를 클릭합니다.



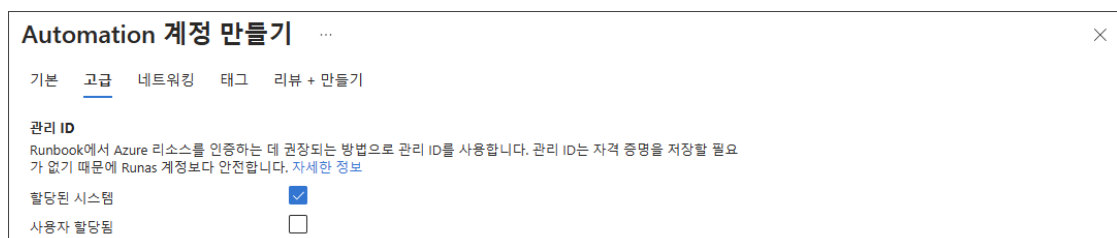
6. [Automation 계정 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.
Log Analytics 작업 영역과 Azure Automation은 서로 매핑되는 지역이 있습니다.

<https://docs.microsoft.com/en-us/azure/automation/how-to/region-mappings> 링크에서 이러한 매핑 지역을 확인할 수 있습니다.

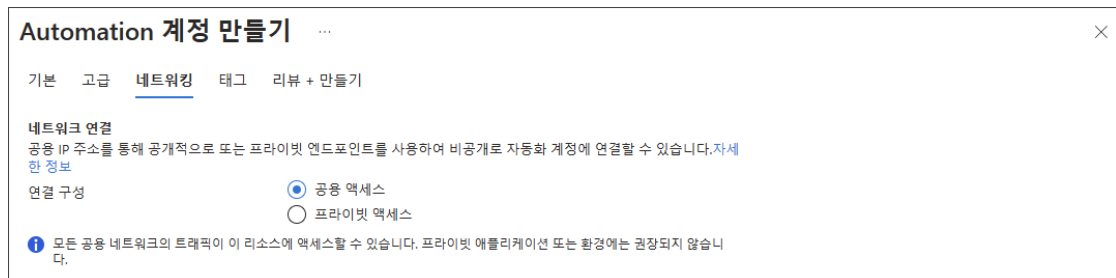
- 리소스 그룹: az104-11-rg1
- [인스턴스 세부 정보 - Automation 계정 이름]: auto<xxxxxxxx> 이름을 입력합니다.
<xxxxxxxx>은 구독 계정 뒤의 숫자를 입력합니다.
- [인스턴스 세부 정보 - 영역]: East US 2



7. [고급] 탭에서 기본값을 유지하고 [다음]을 클릭합니다.



8. [네트워크킹] 탭에서 기본 설정을 유지하고 [리뷰 + 만들기]를 클릭합니다. [리뷰 + 만들기] 탭에서 [만들기]를 클릭합니다.



Automation 계정 만들기 ...

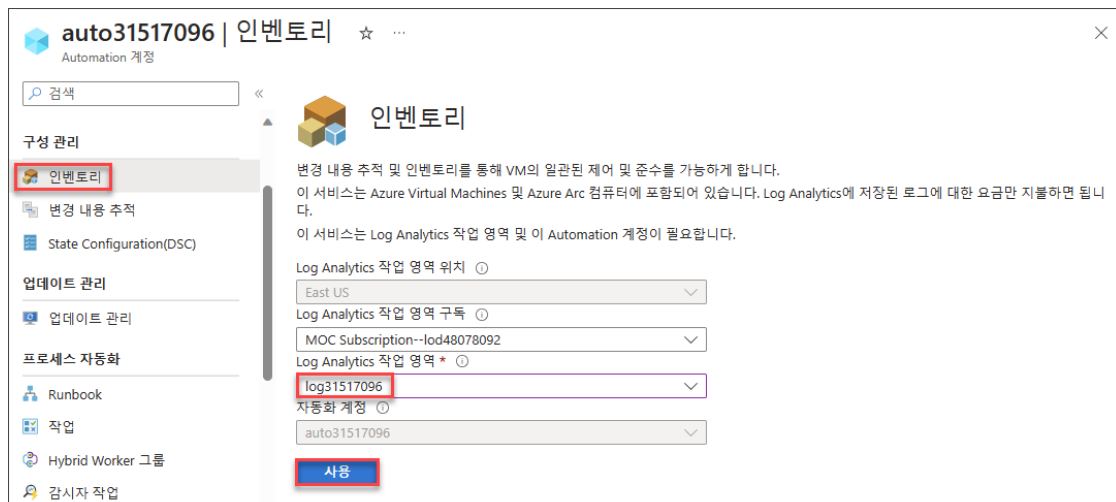
기본 고급 **네트워크킹** 태그 리뷰 + 만들기

네트워크킹 연결
 공용 IP 주소를 통해 공개적으로 또는 프라이빗 엔드포인트를 사용하여 비공개로 자동화 계정에 연결할 수 있습니다. [자세한 정보](#)

연결 구성 ☒ 공용 액세스 ☐ 프라이빗 액세스

모든 공용 네트워크의 트래픽이 이 리소스에 액세스할 수 있습니다. 프라이빗 애플리케이션 또는 환경에는 권장되지 않습니다.

9. 새로 만든 Automation 계정 블레이드로 이동합니다. [Automation 계정] 블레이드의 [구성 관리 - 인벤토리]로 이동한 후 "Log Analytics 작업 영역"에서 앞서 만들었던 작업 영역을 선택하고 [사용]을 클릭합니다.
- 해당 Log Analytics 솔루션의 설치가 완료될 때까지 기다립니다. 완료될 때까지 3분 정도가 소요됩니다.
 - 이렇게 하면 인벤토리 솔루션과 함께 변경 추적(Change tracking) 솔루션도 설치됩니다.



auto31517096 | 인벤토리 ☆ ...

Automation 계정

구성 관리

- 인벤토리**
- 변경 내용 추적
- State Configuration(DSC)

업데이트 관리

- 업데이트 관리

프로세스 자동화

- Runbook
- 작업
- Hybrid Worker 그룹
- 감시자 작업

인벤토리

변경 내용 추적 및 인벤토리를 통해 VM의 일관된 제어 및 준수를 가능하게 합니다. 이 서비스는 Azure Virtual Machines 및 Azure Arc 컴퓨터에 포함되어 있습니다. Log Analytics에 저장된 로그에 대한 요금만 지불하면 됩니다. 이 서비스는 Log Analytics 작업 영역 및 이 Automation 계정이 필요합니다.

Log Analytics 작업 영역 위치

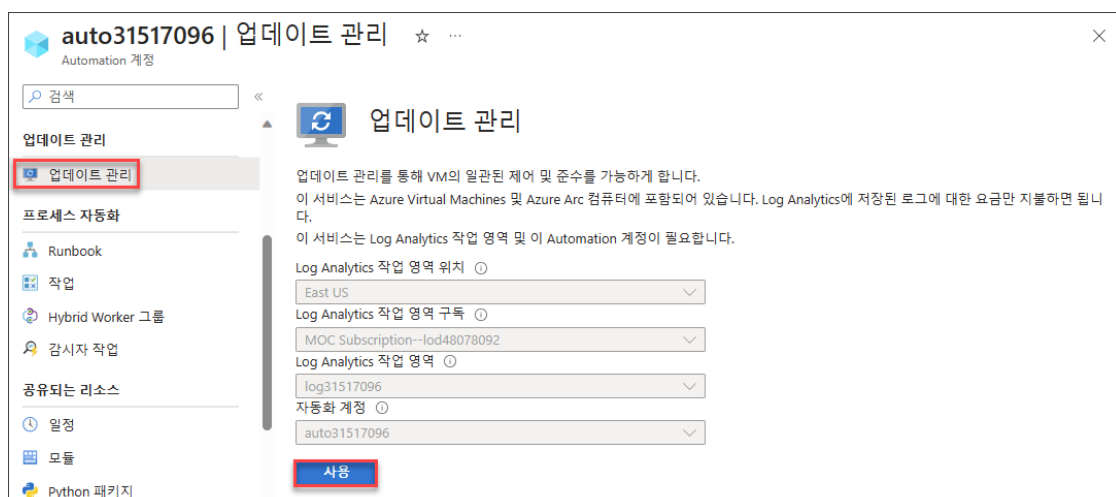
Log Analytics 작업 영역 구독

Log Analytics 작업 영역 *

자동화 계정

사용

10. [Automation 계정] 블레이드의 [업데이트 관리 - 업데이트 관리]로 이동한 후 [사용]을 클릭합니다. 작업이 완료될 때까지 5분 정도가 소요됩니다. 작업이 완료될 때까지 기다립니다.



auto31517096 | 업데이트 관리 ☆ ...

Automation 계정

업데이트 관리

- 업데이트 관리**

프로세스 자동화

- Runbook
- 작업
- Hybrid Worker 그룹
- 감시자 작업

공유되는 리소스

- 일정
- 모듈
- Python 패키지

업데이트 관리

업데이트 관리를 통해 VM의 일관된 제어 및 준수를 가능하게 합니다. 이 서비스는 Azure Virtual Machines 및 Azure Arc 컴퓨터에 포함되어 있습니다. Log Analytics에 저장된 로그에 대한 요금만 지불하면 됩니다. 이 서비스는 Log Analytics 작업 영역 및 이 Automation 계정이 필요합니다.

Log Analytics 작업 영역 위치

Log Analytics 작업 영역 구독

Log Analytics 작업 영역

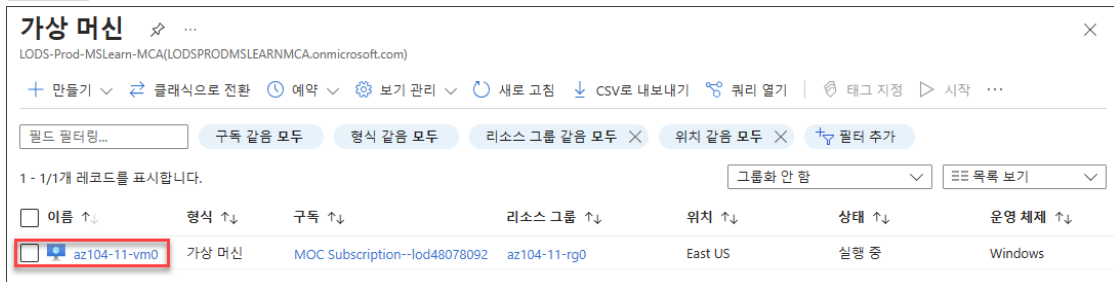
자동화 계정

사용

TASK 04. Azure 가상 머신의 기본 모니터링 설정 검토

이 작업에서는 Azure 가상 머신의 기본 모니터링 설정을 검토합니다.

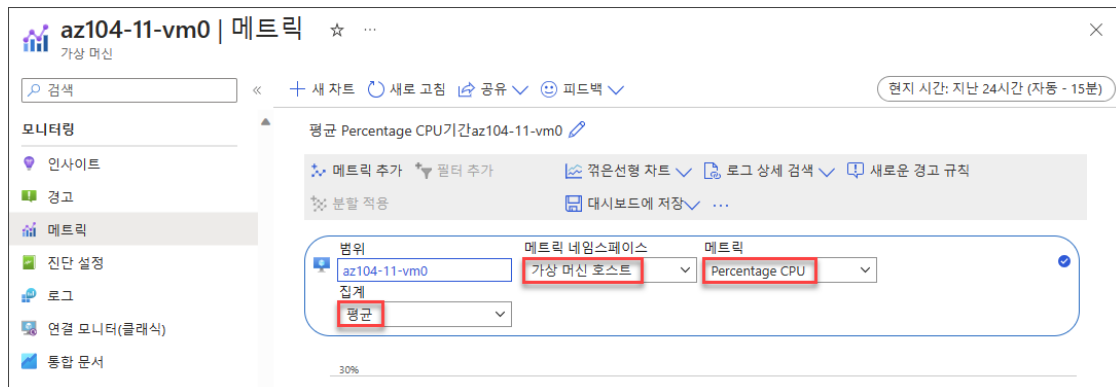
1. Azure 포털의 검색창에서 "가상 머신"을 검색한 후 클릭합니다. [가상 머신] 블레이드에서 **az104-11-vm0** 가상 머신을 클릭합니다.



2. [az104-11-vm0 가상 머신] 블레이드에서 [모니터링 - 메트릭]으로 이동합니다. "메트릭 네임스페이스"에서 "가상 머신 호스트"만 사용할 수 있는 것을 확인합니다.
 - 게스트 수준 진단 설정이 아직 구성되지 않았기 때문에 이는 예상되는 결과입니다.
 - 하지만 메트릭 네임스페이스 드롭다운 목록에서 "게스트 메모리 메트릭 사용"을 직접 설정할 수 있습니다.



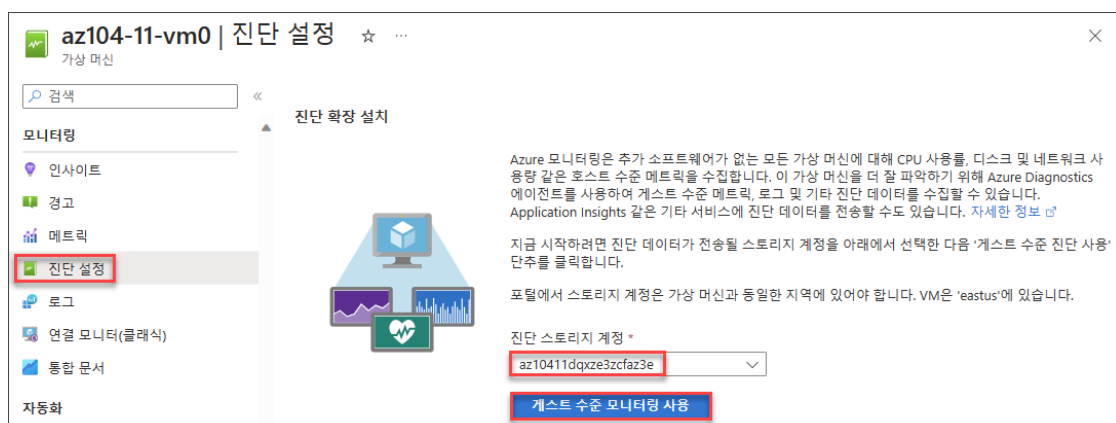
3. [az104-11-vm0 가상 머신] 블레이드의 [모니터링 - 메트릭]에서 "메트릭" 목록을 확장한 후 사용 가능한 메트릭을 확인합니다. "메트릭"은 "Percentage CPU", "집계"는 "평균"을 선택한 후 결과 차트를 검토합니다.
 - 목록에는 게스트 수준 메트릭에 대한 액세스 없이 가상 머신 호스트에서 수집할 수 있는 CPU, 디스크, 네트워크 관련 메트릭 등 다양한 메트릭이 포함되어 있습니다.



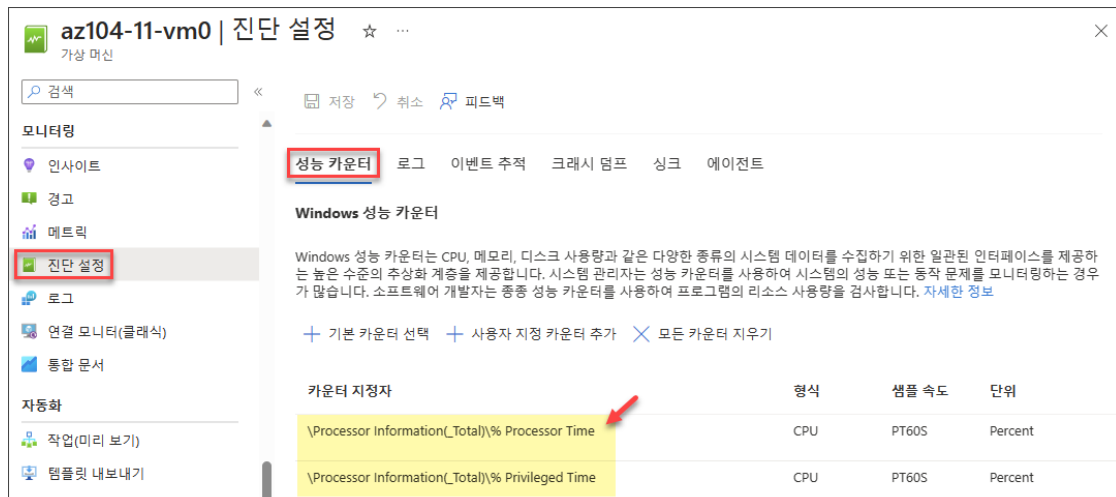
TASK 05. Azure 가상 머신 진단 설정 구성

이 작업에서는 Azure 가상 머신 진단 설정을 구성합니다.

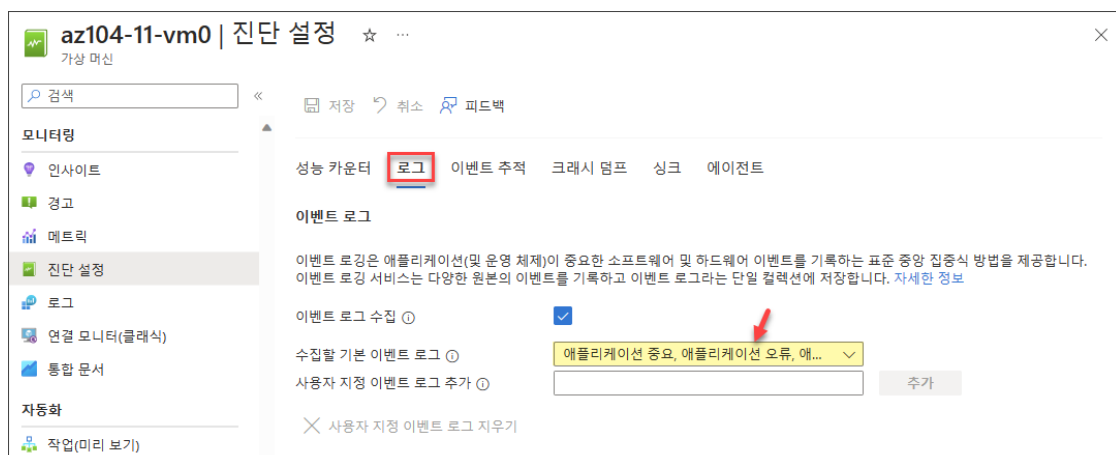
1. [az104-11-vm0 가상 머신] 블레이드의 [모니터링 - 진단 설정]으로 이동합니다. [진단 확장 설치] 페이지에서 "진단 스토리지 계정"을 확장한 후 가상 머신을 만들 때 생성된 스토리지 계정을 선택하고 [게스트 수준 모니터링 사용]을 클릭합니다. 작업은 대략 3분 정도가 소요되며 작업이 완료될 때까지 기다립니다.



2. [az104-11-vm0 가상 머신 | 진단 설정] 블레이드에서 [성능 카운터] 탭으로 이동한 후 사용 가능한 카운터를 검토합니다. 기본적으로 CPU, 메모리, 디스크, 네트워크 카운터를 사용할 수 있습니다. 또한 [사용자 지정]을 선택하여 더 세부적인 목록을 확인할 수도 있습니다.



3. [az104-11-vm0 | 진단 설정] 블레이드의 [로그] 탭으로 이동한 후 사용 가능한 이벤트 로그 컬렉션 목록을 검토합니다. 기본적으로 로그 컬렉션은 보안 로그의 감사 오류뿐 아니라 애플리케이션 로그와 시스템 로그의 위험, 오류, 경고 항목을 포함합니다. 또한 [사용자 지정]을 클릭하여 더 세부적인 구성 설정을 확인할 수 있습니다.



4. [az104-11-vm0 가상 머신] 블레이드의 [모니터링 - 로그]로 이동한 후 [사용]을 클릭합니다.



5. [모니터링 구성] 창에서 아래와 같이 설정한 후 [구성]을 클릭합니다.
 - 다음을 사용하여 인사이트 활성화: Azure Monitor 에이전트

- 구독: 자신의 구독을 선택합니다.
- 데이터 수집 규칙: "새로 만들기" 링크를 클릭합니다.

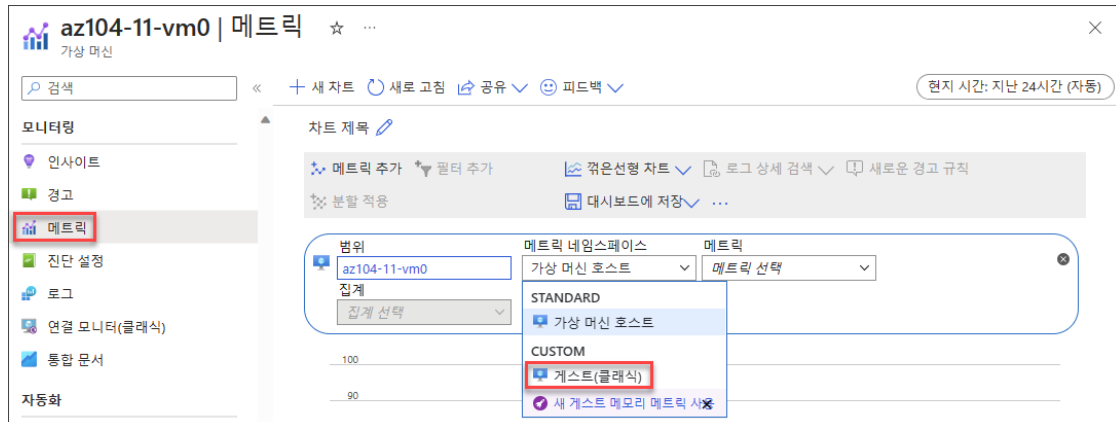
6. [새 규칙 만들기] 창에서 아래와 같이 구성한 후 [만들기]를 클릭합니다.

- 데이터 수집 규칙 이름: az104-collectionRule
- [프로세스 및 종속성 - 프로세스 및 종속성 사용(맵)]: 선택
- [프로세스 및 종속성 - 구독]: 자신의 구독을 선택합니다.
- [프로세스 및 종속성 - Log Analytics workspaces]: 앞서 만들었던 Log Analytics 작업 영역을 선택합니다.

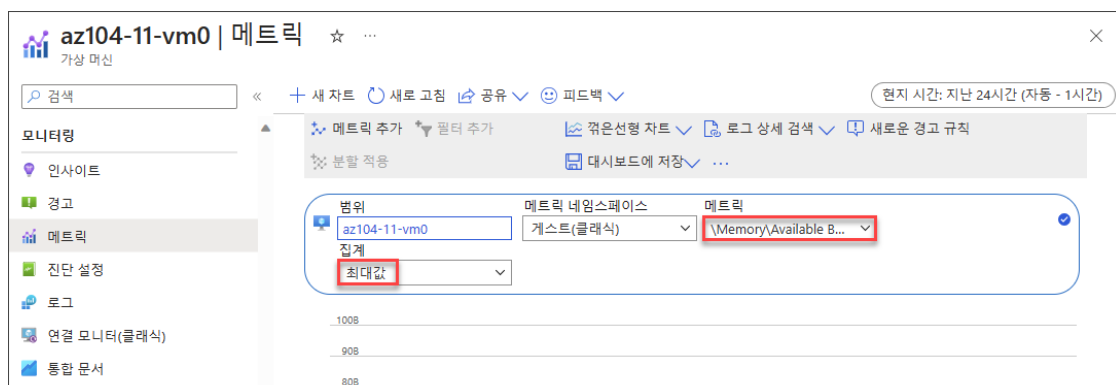
7. [모니터링 구성] 창에서 [구성]을 클릭합니다.

8. [az104-11-vm0 가상 머신] 블레이드의 [모니터링 - 메트릭]으로 이동합니다. "메트릭 네임스페이스"의 드롭다운 목록을 클릭한 후 "가상 머신 호스트" 외에 "게스트(클래식)" 항목이

추가된 것을 확인하고 이를 선택합니다. 앞서 게스트 수준의 진단 설정을 활성화했기 때문에 이제 게스트 수준의 메트릭을 확인할 수 있습니다. 또한 "새 게스트 메모리 메트릭 사용" 옵션도 제공됩니다.



9. [az104-11-vm0 | 메트릭] 블레이드에서 "메트릭" 드롭다운 목록을 확장하여 사용 가능한 메트릭 목록을 확인합니다. "메트릭"은 "\Memory\Available Bytes"를 선택하고 "집계"는 "최대값"을 선택한 후 결과 차트를 확인합니다. 결과가 차트로 표시될 때까지 몇 분의 시간이 소요될 수 있습니다.



TASK 06. Azure Monitor 기능 검토

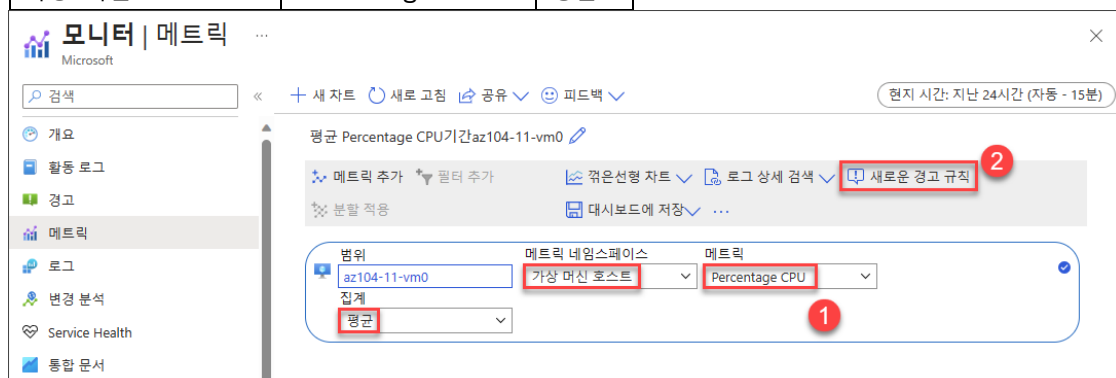
1. Azure 포털의 검색창에서 "모니터"를 검색한 후 클릭합니다. [모니터] 블레이드에서 [메트릭]을 클릭한 후 [범위 선택] 창에서 아래와 같이 구성하고 [적용]을 클릭합니다.
 - 리소스 종류: 가상 머신
 - 위치: 모든 위치
 - 표시된 az104-11-vm0 가상 머신을 선택합니다.



2. [모니터 | 메트릭] 블레이드에서 다음과 같이 선택한 후 [새로운 경고 규칙]을 클릭합니다.

"게스트(클래식)" 메트릭 네임스페이스에서는 메트릭에서 경고 규칙 만들기가 지원되지 않습니다.

메트릭 네임스페이스	메트릭	집계
가상 머신 호스트	Percentage CPU	평균



3. [경고 규칙 만들기] 블레이드의 [조건] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.

- [경고 논리 - 임계값]: 정적
- [경고 논리 - 집계 유형]: 평균
- [경고 논리 - 연산자]: 보다 큼
- [경고 논리 - 임계값]: 2
- [평가할 시기 - 확인 간격]: 1분
- [평가할 시기 - 되돌아보기 기간]: 1분

경고 규칙 만들기 ...

범위 조건 작업 세부 정보 태그 검토 + 만들기

신호를 선택하고 해당 논리를 정의하여 경고 규칙이 트리거되는 시점을 구성합니다.

신호 이름 * ①

[See all signals](#)

경고 논리

임계값 ① ☒ 정적 ☐ 동적

집계 유형 ①

연산자 ①

임계값 * ① %

평가할 시기

확인 간격: ①

되돌아보기 기간 ①

4. [경고 규칙 만들기] 블레이드의 [작업] 탭에서 [작업 그룹 만들기]를 클릭합니다.

경고 규칙 만들기 ...

범위 조건 작업 세부 정보 태그 검토 + 만들기

작업 그룹은 경고 규칙에 적용할 수 있는 작업 집합입니다. [자세한 정보](#)

+ 작업 그룹 선택 **+ 작업 그룹 만들기**

작업 그룹 이름 작업 포함

아직 작업 그룹을 선택하지 않음

5. [작업 그룹 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성하고 [다음]을 클릭합니다.

- [프로젝트 정보 - 리소스 그룹]: az104-11-rg1
- [프로젝트 정보 - 지역]: 전역
- [인스턴스 정보 - 작업 그룹 이름]: az104-11-ag1
- [인스턴스 정보 - 표시 이름]: az104-11-ag1

작업 그룹 만들기 ...

기본 사항 알림 작업 태그 검토 + 만들기

작업 그룹은 경고가 트리거될 때 정의된 알림 및 작업 집합을 호출합니다. [자세한 정보](#)

프로젝트 세부 정보

배포된 리소스와 비용을 관리할 구독을 선택합니다. 풀더 같은 리소스 그룹을 사용하여 모든 리소스를 정리 및 관리합니다.

구독 * ①

리소스 그룹 * ① [새로 만들기](#)

지역 *

인스턴스 정보

작업 그룹 이름 * ①

표시 이름 * ①

표시 이름은 12자로 제한됩니다.

6. [알림] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.

- 알림 유형: 이메일/SMS 메시지/푸시/음성
- 이름: admin email
- [이메일/SMS 메시지/푸시/음성] 창에서 "이메일"을 체크하고 자신의 메일 주소를 입력한 후 [확인]을 클릭합니다.

7. [작업] 탭에서 "작업 유형" 드롭다운 목록을 확장하여 어떤 작업을 수행할 수 있는지 확인합니다. 아무런 설정도 하지 않고 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

8. [경고 규칙 만들기] 블레이드의 [작업] 탭이 다시 표시됩니다. 앞서 추가한 작업 그룹이 표시되는 것을 확인하고 [다음]을 클릭합니다.

9. [경고 규칙 만들기] 블레이드의 [세부 정보] 탭에서 아래와 같이 구성하고 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
- [프로젝트 정보 - 리소스 그룹]: az104-11-rg1
 - [경고 규칙 세부 정보 - 심각도]: 3- 정보
 - [경고 규칙 세부 정보 - 경고 규칙 이름]: CPU Percentage above the test threshold
 - [경고 규칙 세부 정보 - 경고 규칙 설명]: CPU Percentage above the test threshold
 - [경고 규칙 세부 정보 - 고급 옵션 - 설정]: "만들어지면 바로 사용", "자동으로 경고 해결"

옵션을 모두 선택합니다.

경고 규칙 만들기 ...

범위 조건 작업 세부 정보 태그 검토 + 만들기

프로젝트 정보
경고 규칙을 저장할 구독 및 리소스 그룹을 선택합니다.

구독 * ① MOC Subscription--lod48078092

리소스 그룹 * ① az104-11-rg1
새로 만들기

경고 규칙 세부 정보

심각도 * ① 3 - 정보

경고 규칙 이름 * ① CPU Percentage above the test threshold ✓

경고 규칙 설명 ① CPU Percentage above the test threshold

고급 옵션
설정

만들어지면 바로 사용 ① ☒

자동으로 경고 해결 ① ☒

10. 메트릭 경고 규칙이 활성화될 때까지 최대 10분이 소요됩니다.

11. Azure 포털의 검색창에서 "가상 머신"을 검색한 후 클릭합니다. [가상 머신] 블레이드에서 az104-11-vm0 가상 머신을 클릭합니다.

가상 머신 ...

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

+ 만들기 > < 클래식으로 전환 < 예약 < 보기 관리 < 새로 고침 < CSV로 내보내기 < 쿼리 열기 < 태그 지정 < 시작 ...

필드 필터링... 구독 있음 모두 형식 있음 모두 리소스 그룹 있음 모두 위치 있음 모두 < 필터 추가

1 - 1/1개 레코드를 표시합니다. 그룹화 안 함 목록 보기

<input type="checkbox"/>	이름 ↑↓	형식 ↑↓	구독 ↑↓	리소스 그룹 ↑↓	위치 ↑↓	상태 ↑↓	운영 체제 ↑↓
<input checked="" type="checkbox"/>	az104-11-vm0	가상 머신	MOC Subscription--lod48078092	az104-11-rg0	East US	실행 중	Windows

12. [az104-11-vm0 가상 머신] 블레이드의 [설정 - 연결]로 이동한 후 [RDP 파일 다운로드]를 클릭합니다. 다운로드 받은 파일을 실행하고 사용자 이름(Student), 암호(Pa55w.rd1234)를 사용하여 가상 머신에 로그인합니다.

az104-11-vm0 | 연결 ...

가상 머신

검색

설정

네트워킹

연결

Windows Admin Center

디스크

크기

클라우드용 Microsoft Defender

Advisor 권장 사항

확장 프로그램 + 애플리케이션

가용성 + 크기 조정

구성

ID

보안을 강화하려면 이 VM에서 Just-In-Time 액세스를 활성화하세요. →

RDP SSH Bastion

RDP를 사용하여 연결

권장 연결 방법

Azure는 이 방법을 사용하여 연결할 때 가장 일반적인 필수 구성 요소의 상태를 확인했습니다.

- 클라이언트의 IP 주소에서 들어오는 인바운드 액세스에 대해 네트워크 보안 그룹을 확인합니다. [자세한 정보](#)
- VM의 네트워크 인터페이스에는 공용 IP 주소가 있습니다. [자세한 정보](#)
- VM이 실행 중입니다.

RDP를 통해 가상 머신에 연결하려면 IP 주소를 선택하고 필요에 따라 포트 번호를 변경하고 RDP 파일을 다운로드합니다.

IP 주소 * 공용 IP 주소(20.231.9.16)

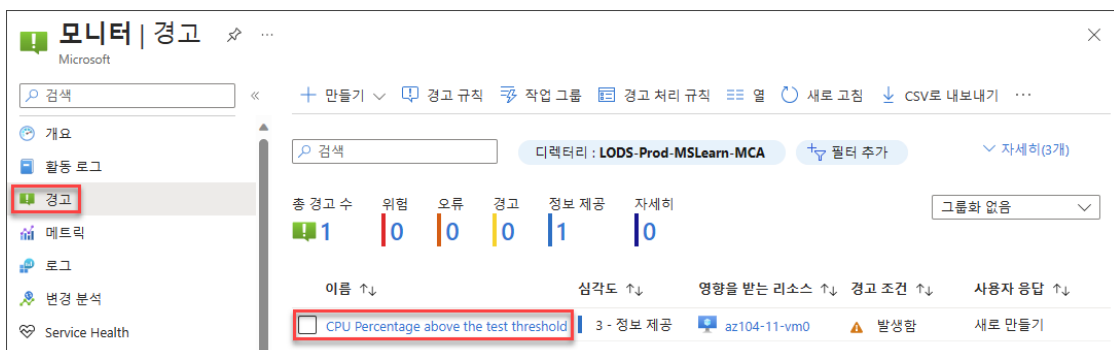
포트 번호 * 3389

RDP 파일 다운로드

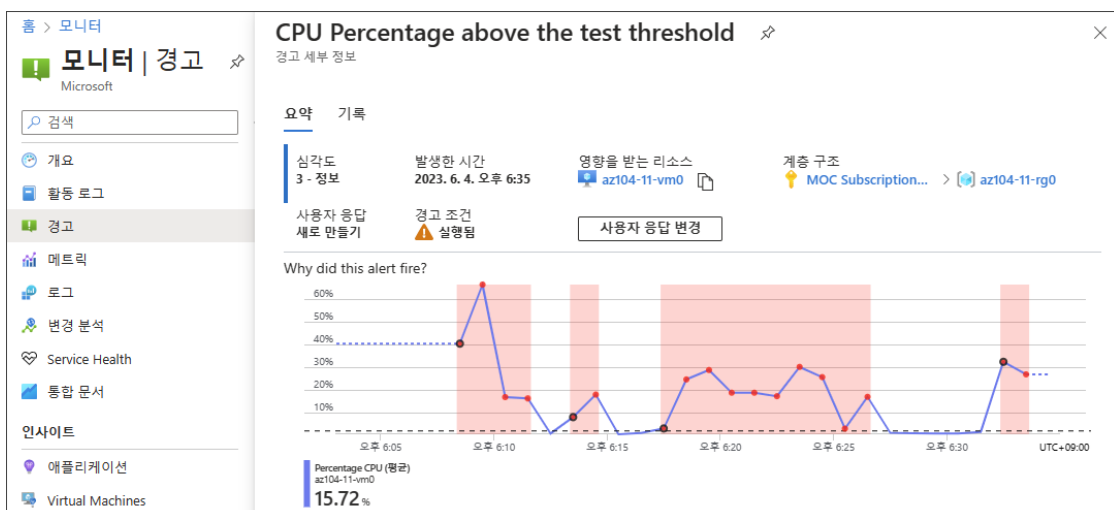
13. az104-11-vm0 가상 머신에서 명령 프롬프트를 열고 다음 명령을 실행하여 CPU 사용률을 증가시킵니다. 이 명령은 새로 만든 경고 규칙 임계값 이상으로 CPU 사용률을 증가시키는 무한 루프가 시작됩니다.

```
# CPU 사용량 증가
for /l %a in (0,0,1) do echo a
```

14. Azure 포털의 네비게이션 메뉴에서 [모니터]를 클릭합니다. [모니터] 블레이드의 [경고]로 이동합니다. "CPU Percentage above the test threshold" 이름의 경고가 생성된 것을 확인하고 이를 클릭합니다.



15. [모니터 | 경고] 블레이드에서 경고 세부 정보를 확인합니다.



16. az104-11-vm0 가상 머신으로 전환한 후 실행 중인 CMD 창을 닫습니다.

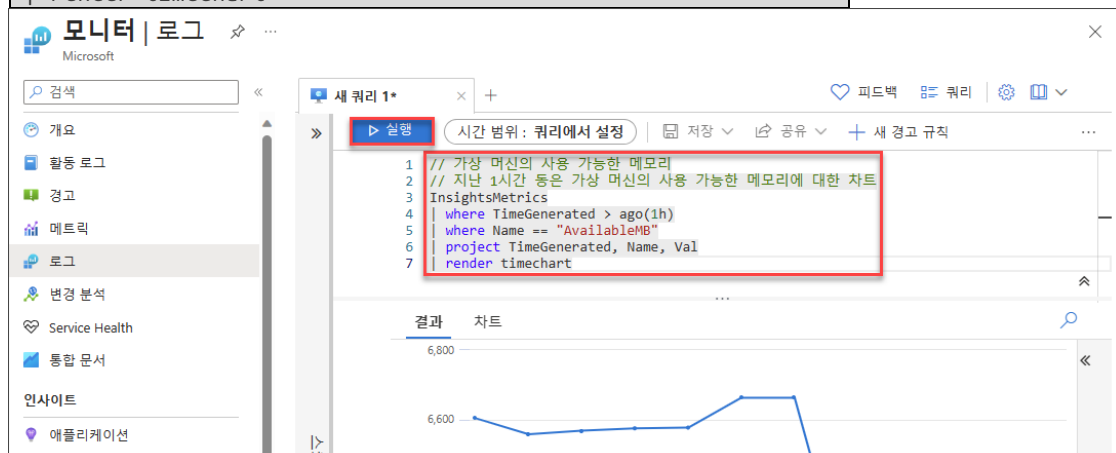
TASK 07. Azure Log Analytics 기능 검토

1. [모니터] 블레이드에서 [로그]로 이동합니다. [Log Analytics 시작] 창이 표시되면 창을 닫습니다. [범위 선택] 창의 [찾아보기] 탭에서 리소스 종류를 "가상 머신"으로 선택합니다. az104-11-vm0 가상 머신을 선택한 후 [적용]을 클릭합니다.

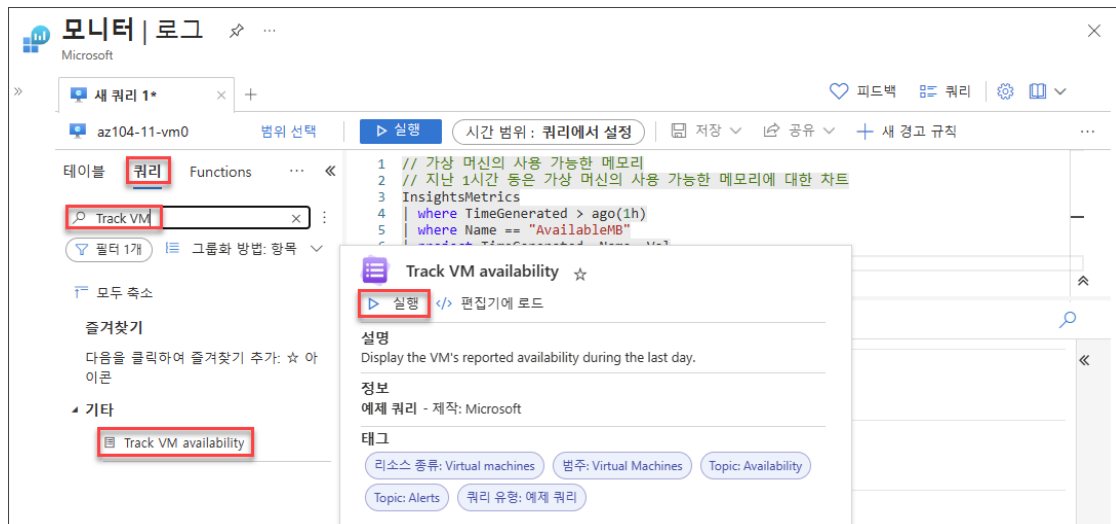


2. [새 쿼리] 탭의 쿼리창에 다음과 같은 쿼리를 작성한 후 [실행]을 클릭합니다. 출력된 차트 내용을 검토합니다.

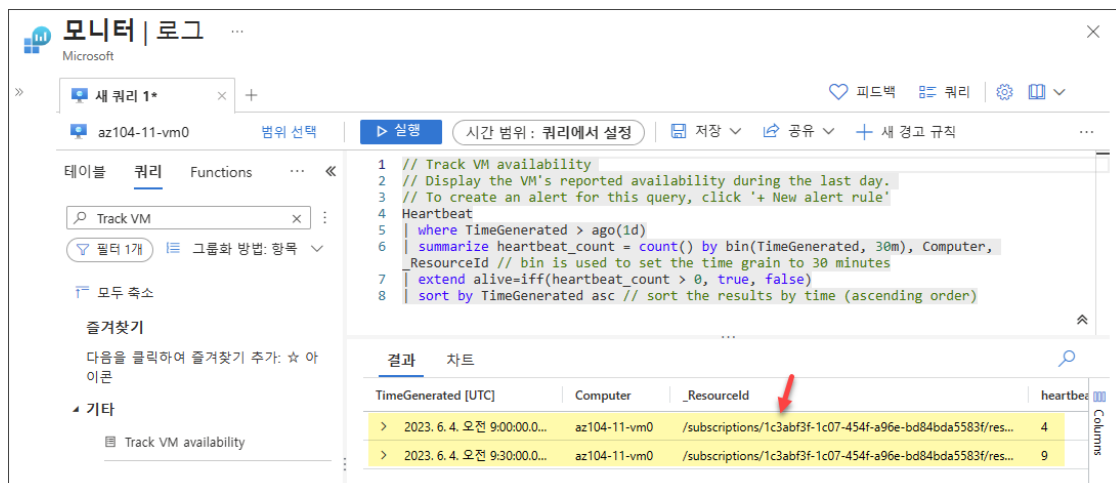
```
// 가상 머신의 사용 가능한 메모리
// 지난 1시간 동안 가상 머신의 사용 가능한 메모리에 대한 차트
InsightsMetrics
| where TimeGenerated > ago(1h)
| where Name == "AvailableMB"
| project TimeGenerated, Name, Val
| render timechart
```



3. [스키마 및 필터] 영역에서 [쿼리] 탭으로 이동한 후 "Track VM"을 검색합니다. 검색한 "Track VM availability"로 마우스를 이동한 후 [Track VM availability] 타일의 [실행]을 클릭합니다.



4. 쿼리 창에 새 쿼리가 실행되고 결과가 테이블로 출력됩니다. 출력된 내용을 검토합니다.



5. [스키마 및 필터] 영역의 [테이블] 탭으로 이동합니다. "Virtual machines" 섹션에서 표시되는 여러 로그 테이블을 검토합니다. 일부 테이블의 이름은 이 실습 초기에 설치한 솔루션의 이름과 일치하는 것을 확인할 수 있습니다. "VMComputer" 테이블로 마우스를 이동한 후 표시되는 창에서 [미리 보기 데이터 참조]를 클릭합니다.

The screenshot shows the Microsoft Monitor Logs interface. On the left, the 'Virtual machines' section is expanded, and 'VMComputer' is selected. The main area displays a Kusto query:

```
1 // Track VM availability
2 // Display the VM's reported availability during the last day.
3 // To create an alert for this query, click '+ New alert rule'
4 Heartbeat
5 | where TimeGenerated > ago(1d)
6 | summarize heartbeat_count = count() by bin(TimeGenerated, 30m), Computer,
7   ResourceId // bin is used to set the time grain to 30 minutes
8 | extend alive-iff(heartbeat_count > 0, true, false)
9 | sort by TimeGenerated asc // sort the results by time (ascending order)
```

Below the query, a table titled 'VMComputer' is shown. It has two columns: 'Computer' and 'heartbeat_count'. The table contains two rows of data:

Computer	heartbeat_count
54f-a96e-bd84bda5583f/res...	4
54f-a96e-bd84bda5583f/res...	9

A red box highlights the 'VMComputer' table name in the left sidebar, and another red box highlights the '미리 보기 데이터 참조' (Preview data reference) link in the table's description.

6. [VMComputer] 창에서 데이터가 해당 테이블의 데이터가 표시되는지 확인합니다.

The screenshot shows the Microsoft Monitor Logs interface with the 'VMComputer' table selected. The table is displayed with the following data:

TimeGenerated [UTC]	Computer
2023. 6. 4. 오전 9:25:15.880	az104-11-vm0

A red arrow points to the 'Computer' column header, indicating the data being displayed.

TASK 08. 리소스 정리

1. [Cloud Shell]에서 PowerShell을 열고 다음 명령을 실행하여 이 실습에서 만든 모든 리소스 그룹을 확인합니다.

```
# 실습에서 사용한 리소스 그룹 확인
Get-AzResourceGroup -Name 'az104-11*'

```

```
PowerShell
PS /home/labuser-31517096> # 실습에서 사용한 리소스 그룹 확인
PS /home/labuser-31517096> Get-AzResourceGroup -Name 'az104-11*'

ResourceGroupName : az104-11-rg0
Location           : eastus
ProvisioningState   : Succeeded
Tags               :
ResourceId          : /subscriptions/1c3abf3f-1c07-454f-a96e-bd84bda5583f/resourceGroups/az104-11-rg0

ResourceGroupName : az104-11-rg1
Location           : eastus
ProvisioningState   : Succeeded
Tags               :
ResourceId          : /subscriptions/1c3abf3f-1c07-454f-a96e-bd84bda5583f/resourceGroups/az104-11-rg1
```

2. [Cloud Shell]에서 다음 명령을 실행하여 실습에서 만든 모든 리소스 그룹을 삭제합니다. 이 명령은 `-AsJob` 매개 변수로 인해 비동기적으로 실행되므로 PowerShell 세션 내에서 다른 PowerShell 명령을 즉시 실행할 수 있지만 리소스 그룹이 실제로 삭제될 때까지는 몇 분 정도 걸립니다.

```
# 실습에서 사용한 리소스 그룹 삭제
Get-AzResourceGroup -Name 'az104-11*' | Remove-AzResourceGroup -Force -AsJob

PowerShell
PS /home/labuser-31517096> # 실습에서 사용한 리소스 그룹 삭제
PS /home/labuser-31517096> Get-AzResourceGroup -Name 'az104-11*' | Remove-AzResourceGroup -Force -AsJob

Id      Name      PSJobTypeName State      HasMoreData Location      Command
--      -
2      Long Running 0_ AzureLongRunni_ Running    True        localhost    Remove-AzResourceGroup
3      Long Running 0_ AzureLongRunni_ Running    True        localhost    Remove-AzResourceGroup

PS /home/labuser-31517096>
```