



Microsoft Cloud Workshop

Azure Monitoring 101

Hands-on lab step-by-step

Lab

Oct 2018

Min Ae Cho (CSA)

Contents

Monitoring 101.....	1
hands-on lab.....	1
step-by-step.....	1
목표	1
Lab 구성.....	2
요구사항	2
Lab 1. Azure Log Analytics	3
Step 1: Azure Log Analytics 설치 및 구성	4
Step 2: Azure Log Analytics 에 리소스 연결하기 (VM Agent 가 설치되어 있는 경우)	6
Step 2.1: Azure Log Analytics 에 리소스 연결하기 (VM Agent 가 설치되어 있지 않은 경우).....	8
Lab 2. Azure 로그 분석(Log Analytics) 사용하기	15
Lab 3. Azure 보안 센터(Security Center) 사용하기	24

Monitoring 101

hands-on lab

step-by-step

목표

Azure 에서 제공하는 모니터링 솔루션(Log Analytics, OMS)을 사용하여 다양한 환경(온프레미스, 클라우드) 의 리소스들을 효율적으로 한 곳에서 모니터링하고 보안 센터(Security Center)를 이용하여 보안을 중점적으로 모니터링하고 외부의 위협을 감지해 더 안전한 보안 아키텍처를 구성할 수 있게 한다.

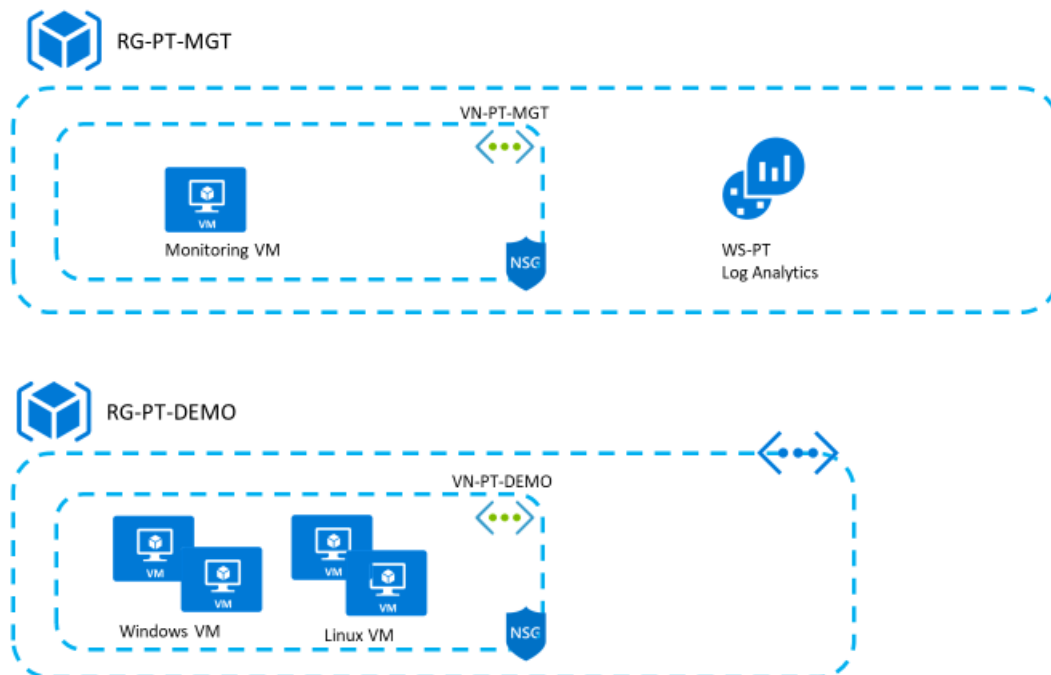
사용하는 Azure 서비스

- Azure 가상머신
- Azure Log Analytics , OMS
- Azure 보안센터 (Security Center)

Lab 구성

PowerShell 을 이용해 배포한 가상 머신들에 Log Analytics 를 사용할 수 있게 OMS agent 설치와 구성을 진행한다.

1. 리소스 그룹 : 관리용(MGT), 서비스용(PRD) 용도 두개의 리소스 그룹 구성
2. 가상 네트워크 : 두개의 격리된 논리 네트워크 구성
3. 가용성 집합 : 가상머신 가용성 집합 구성
4. 네트워크 보안 그룹 : 네트워크 필터링을 위한 보안 그룹 구성
5. Azure Log Analytics : OMS Agent 기반 데이터들을 저장하고 쿼리할 수 있게 하는 서비스



요구사항

- Microsoft Azure subscription
- Local machine
- Lab 1 – 2 실습

Lab 1. Azure Log Analytics

크게 두가지의 시나리오를 가지고(agent 가 설치되어 있지 않은 경우, 설치된 경우) Log Analytics 를 사용할 수 있는 방법에 대해 알아보고 실습해봅니다.

Microsoft Azure VM Agent 는 Azure 패브릭 컨트롤러와 가상 머신의 상호 작용을 관리하는 안전하고 간단한 프로세스입니다. 가상 머신 Agent 는 가상 머신 확장(VM Extension)을 설정하고 실행하는 데 기본적인 역할을 수행합니다. 가상 머신 확장(Virtual Machine Extension)을 사용하면 소프트웨어 설치 및 구성과 같은 가상 머신 배포 후 구성을 설정할 수 있습니다. Azure VM Agent 가 없으면 가상 머신 확장을 실행할 수 없습니다. 또한 Azure Backup 또는 Azure Security 와 같은 일부 Azure 서비스를 이용할 수 없기 때문에 설치를 권장합니다.

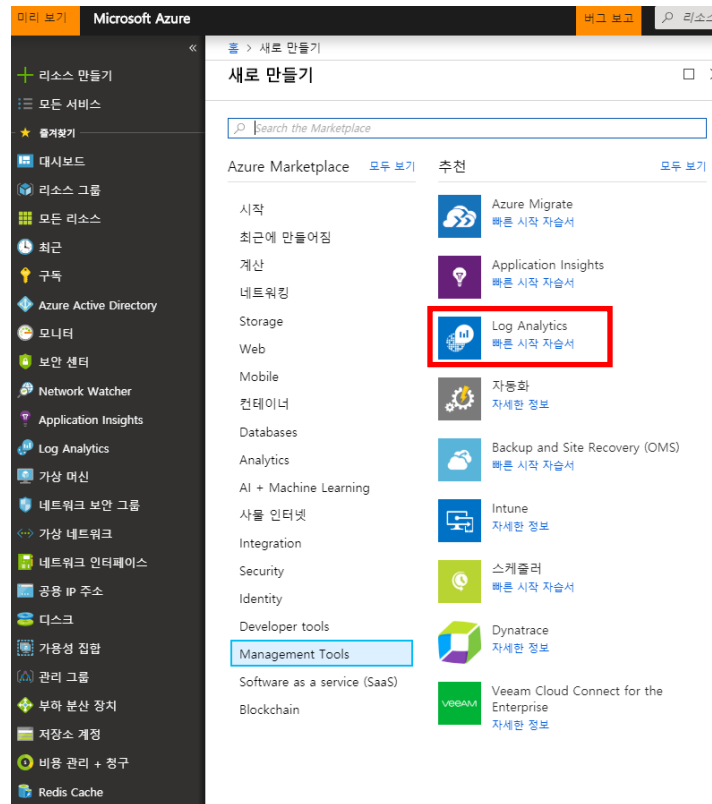
Azure VM Agent 는 Azure Marketplace 이미지에서 배포된 모든 Windows VM 에 기본적으로 설치됩니다. Azure Portal, PowerShell, 명령줄 인터페이스(Command Line Interface: CLI) 또는 Azure Resource Manager 템플릿에서 Azure Marketplace 이미지를 배포하면 Azure VM Agent 도 자동적으로 설치됩니다.

Azure VM Agent 의 Windows Guest Agent 패키지는 두 부분으로 나누어있습니다.

- PA(Provision Agent) : VM 을 부팅하려면 VM 에 PA 가 설치되어 있어야합니다.
- WinGA (Windows Guest Agent)

Step 1: Azure Log Analytics 설치 및 구성

1. Azure 포털에서 "리소스 만들기"를 선택 후 "Management Tools"를 선택합니다.
우측에 나오는 서비스 중 Log Analytics 를 선택합니다.



2. "새로 만들기" 버튼을 클릭하여 로그 분석 작업 영역을 생성합니다.

로그 분석 작업 영역 □ ×

새로 만들거나 OMS 포털에서 만들어진 기존 항목...

☒ 새로 만들기 ☐ 기존 연결

* OMS 작업 영역 ⓘ

WS-PT ✓

* 구독

minaecho-CSA ▼

* 리소스 그룹 ⓘ

☐ 새로 만들기 ☒ 기존 그룹 사용

RG-PT-MGT ▼

* 위치

아시아 남동부 ▼

* 가격 책정 계층

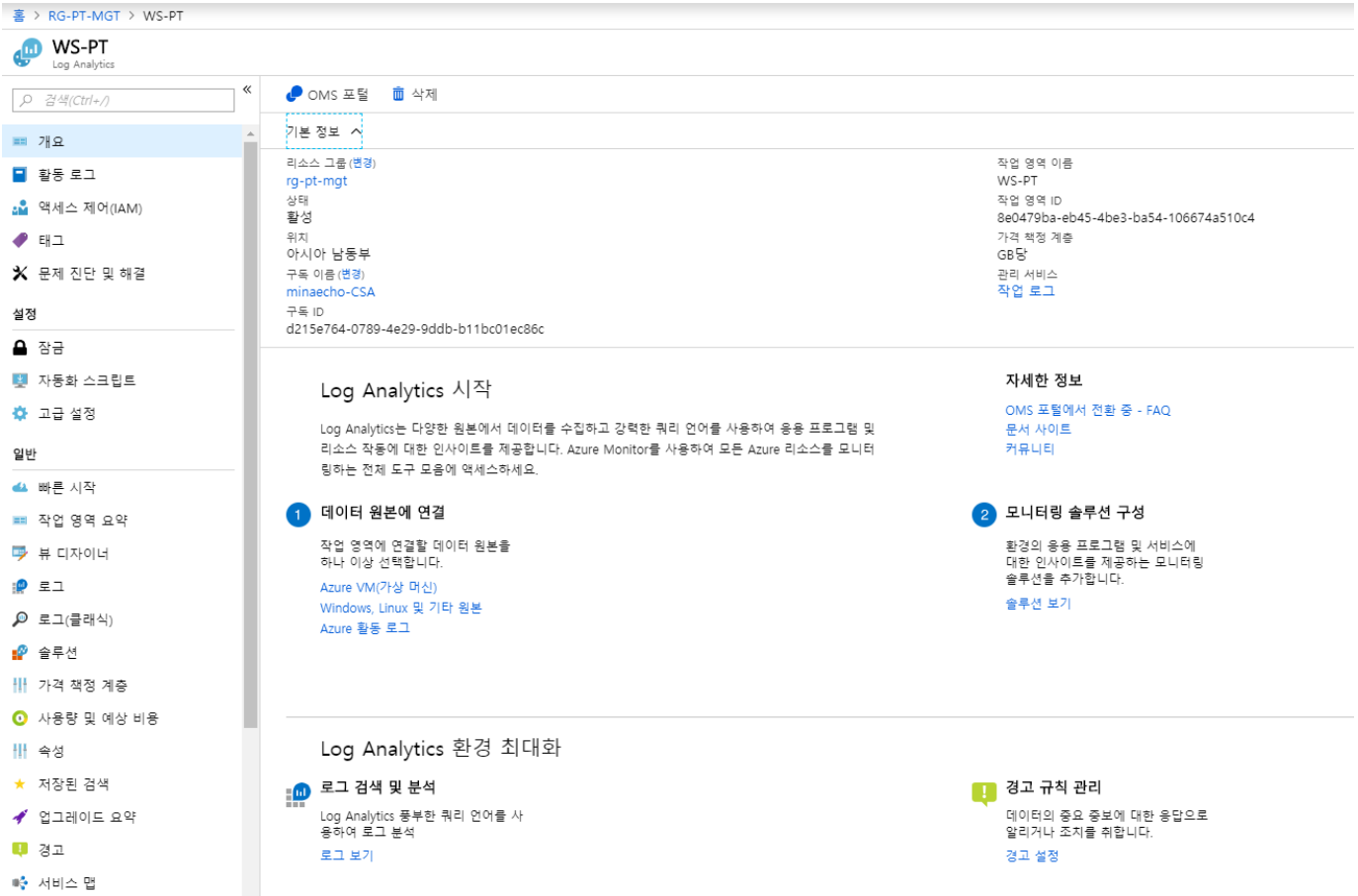
GB당 >

구독 : 사용할 구독 계정 선택

리소스 그룹 : 기존 위치 사용 선택 후 RG-PT-MGT 선택

위치 : 아시아 남동부

3. 아래와 같이 리소스 그룹에 (RG-PT-MGT) 로그 분석(Log Analytics) 리소스가 생성된 것을 확인합니다.



홈 > RG-PT-MGT > WS-PT

WS-PT
Log Analytics

OMS 포털 삭제

기본 정보

리소스 그룹 (변경)
rg-pt-mgt
상태
활성
위치
아시아 남동부
구독 이름 (변경)
minaecho-CSA
구독 ID
d215e764-0789-4e29-9ddb-b11bc01ec86c

작업 영역 이름
WS-PT
작업 영역 ID
8e0479ba-eb45-4be3-ba54-106674a510c4
가격 책정 계층
GB당
관리 서비스
작업 로그

Log Analytics 시작

Log Analytics는 다양한 원본에서 데이터를 수집하고 강력한 쿼리 언어를 사용하여 응용 프로그램 및 리소스 작동에 대한 인사이트를 제공합니다. Azure Monitor를 사용하여 모든 Azure 리소스를 모니터링하는 전체 도구 모음에 액세스하세요.

자세한 정보
[OMS 포털에서 전환 중 - FAQ](#)
[문서 사이트](#)
[커뮤니티](#)

1 데이터 원본에 연결

작업 영역에 연결할 데이터 원본을 하나 이상 선택합니다.

[Azure VM\(가상 머신\)](#)
[Windows, Linux 및 기타 원본](#)
[Azure 활동 로그](#)

2 모니터링 솔루션 구성

환경의 응용 프로그램 및 서비스에 대한 인사이트를 제공하는 모니터링 솔루션을 추가합니다.

[솔루션 보기](#)

Log Analytics 환경 최적화

로그 검색 및 분석

Log Analytics 풍부한 쿼리 언어를 사용하여 로그 분석

[로그 보기](#)

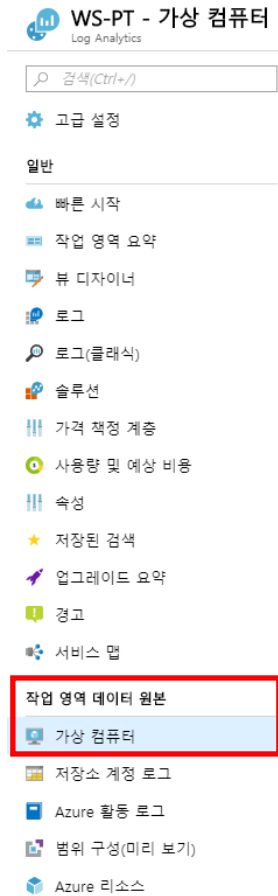
경고 규칙 관리

데이터의 중요 정보에 대한 응답으로 알리거나 조치를 취합니다.

[경고 설정](#)

Step 2: Azure Log Analytics 에 리소스 연결하기 (VM Agent 가 설치되어 있는 경우)

1. Log Analytics 서비스로 이동하여, "작업 영역 데이터 원본" 에서 가상 컴퓨터 버튼을 클릭합니다.

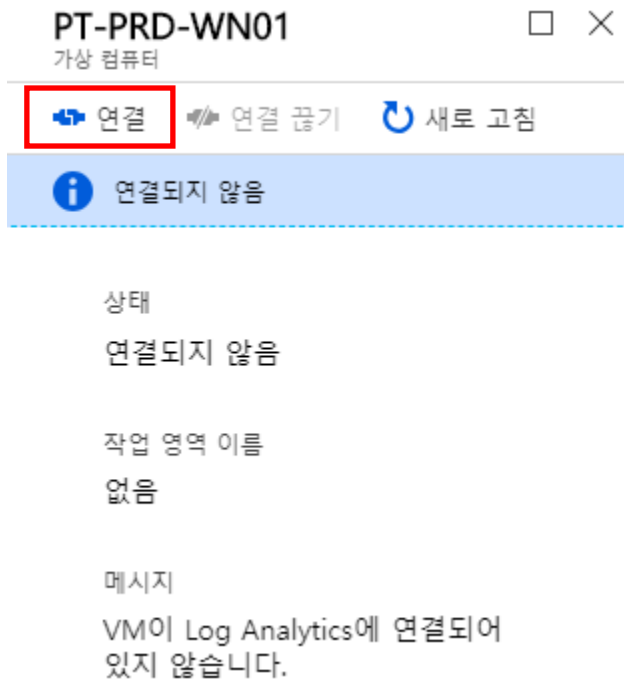


"가상 컴퓨터" 버튼을 누르면 현재 구독에 있는 가상 컴퓨터 목록이 보이며 OMS 연결 여부가 표시됩니다.

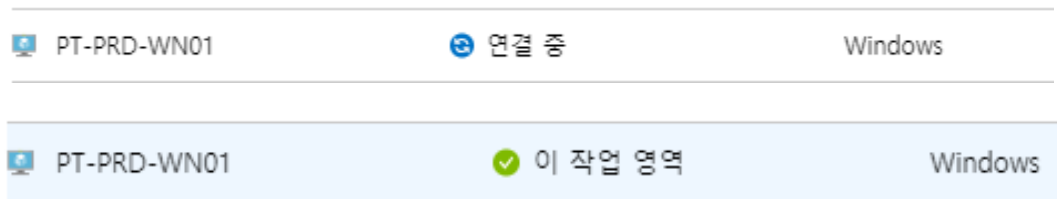
새로 고침 ? 도움말

이름으로 필터링...	8개 선택됨	2개 선택됨	minaecho-CSA	8개 선택됨	3개 선택됨
이름	OMS 연결	OS	구독	리소스 그룹	위치
MSFT-HKG-VM01	다른 작업 영역	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	MSFT-GamePod-RG	eastasia
PT-MGT-MSM01	연결되지 않음	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	RG-PT-MGT	koreacentral
PT-PRD-LX01	연결되지 않음	Linux	d215e764-0789-4e29-9ddb-b11bc01ec86c	RG-PT-DEMO	koreacentral
PT-PRD-LX02	연결되지 않음	Linux	d215e764-0789-4e29-9ddb-b11bc01ec86c	RG-PT-DEMO	koreacentral
PT-PRD-WN01	연결되지 않음	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	RG-PT-DEMO	koreacentral
PT-PRD-WN02	연결되지 않음	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	RG-PT-DEMO	koreacentral
pt-test-vm01	다른 작업 영역	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	pt-test-rg	koreacentral
Srv-IIS01	다른 작업 영역	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	SC-RIG	southeastasia
Srv-IIS02	다른 작업 영역	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	SC-RIG	southeastasia
Srv-Jump	다른 작업 영역	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	SC-RIG	southeastasia
Srv-Work	다른 작업 영역	Windows	d215e764-0789-4e29-9ddb-b11bc01ec86c	SC-RIG	southeastasia

2. 연결하려는 가상 머신을 선택합니다. (PT-PRD-WN01) 선택 후 “연결” 버튼을 누릅니다.



실행 중이면 다음과 같은 화면이 나오게 됩니다. 가상머신이 실행 중이지 않거나 Azure VM Agent 가 설치되지 않았다면 “오류”가 나타납니다.



가상 머신 Agent 가 설치되었다면 Linux 가상 머신도 동일한 방법으로 연결이 가능합니다.

Step 2.1: Azure Log Analytics 에 리소스 연결하기 (VM Agent 가 설치되어 있지 않은 경우)

Azure Marketplace 를 통해 가상 머신을 생성하거나 Azure Resource Manager Template, PowerShell, CLI 을 이용해서 가상머신을 생성할때 VM Agent 설치를 함께 한다면 VM Agent 는 자동으로 설치되어 있습니다.

그러나 Custom VHD 를 이용해 가상 머신을 생성하거나 VM Agent 를 설치하지 않았을 때의 Log Analytics 설정 방법에 대해 알아봅니다. Log Analytics 리소스 생성은 전과 동일하여 생략합니다.

1.VM Agent 가 설치되지 않은 가상 컴퓨터에 접속합니다. (ex. 윈도우 : RDP, 리눅스 : SSH 이용)

현재 실습은 윈도우를 기반으로 진행됩니다.

해당 URL 사이트로 이동합니다.

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/agent-windows>

수동 설치

Windows VM 에이전트는 Windows 설치 관리자 패키지를 사용하여 수동으로 설치할 수 있습니다. Azure에 배포된 사용자 지정 VM 이미지를 만들 때 수동 설치가 필요할 수 있습니다. Windows VM 에이전트를 수동으로 설치하려면 [VM 에이전트 설치 관리자를 다운로드합니다.](#)

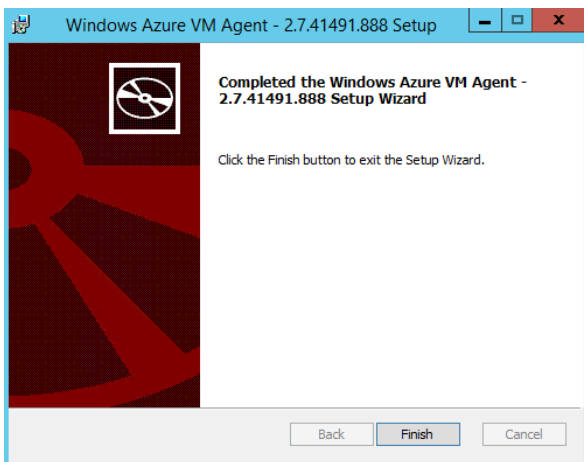
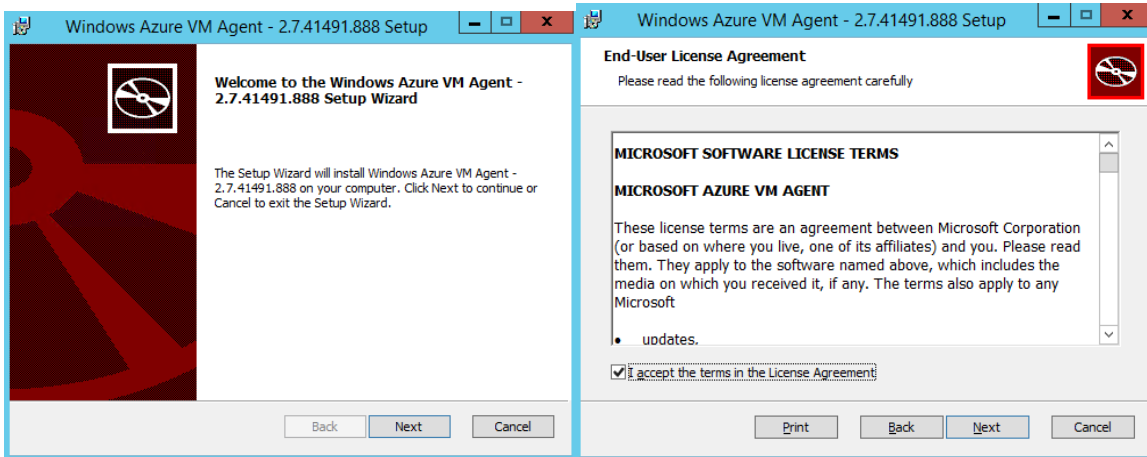
VM 에이전트는 Windows 설치 관리자 파일을 두 번 클릭하여 설치할 수 있습니다. VM 에이전트를 자동 또는 무인으로 설치하려면 다음 명령을 실행합니다.

cmd

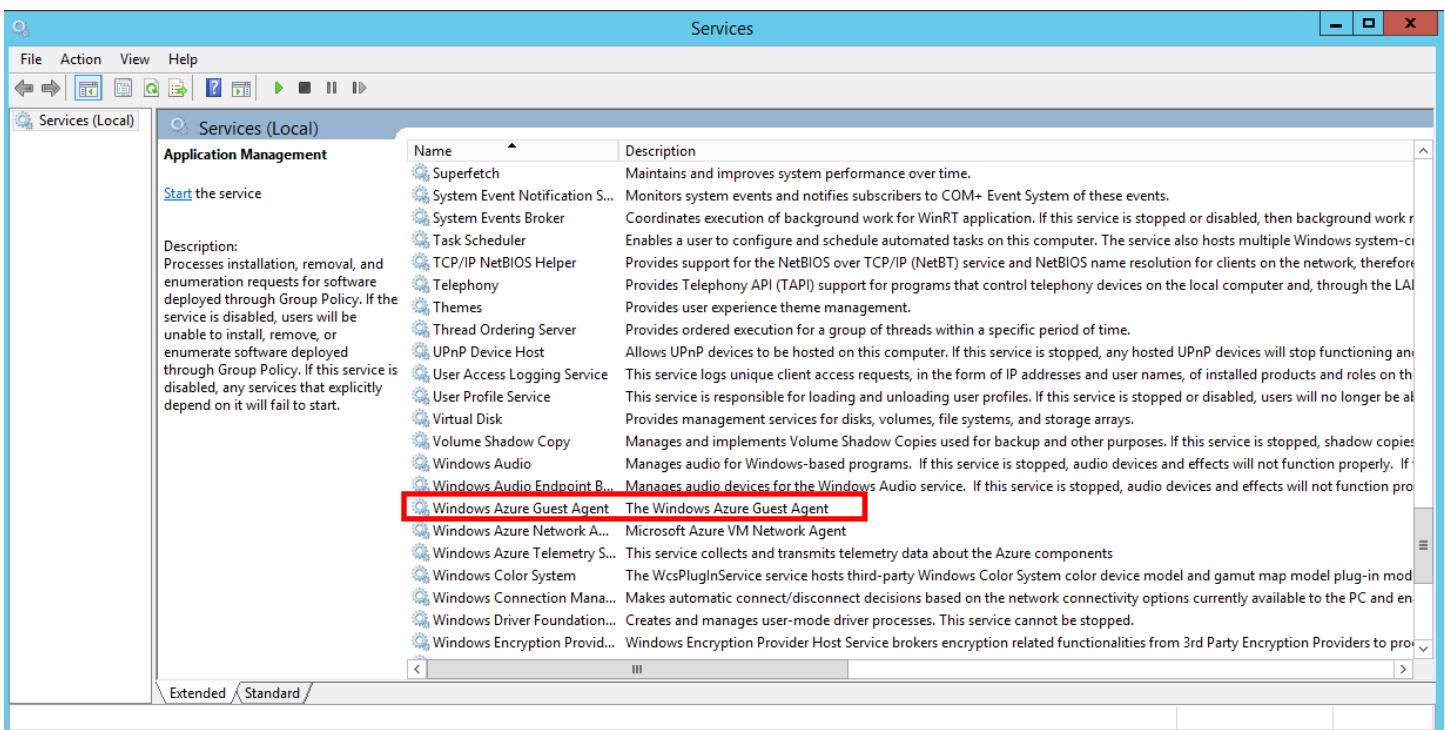
복사

```
msiexec.exe /i WindowsAzureVmAgent.2.7.1198.778.rd_art_stable.160617-1120.fre /quiet
```

설치에는 두가지 방법이 있으며 url 을 통한 다운로드 방법 혹은 CMD 를 이용한 방법이 있습니다.

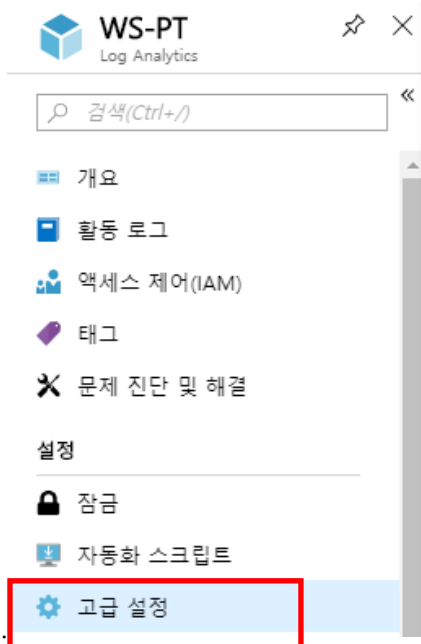


설치가 완료되면 “Services”에서 다음과 같은 Agent 를 확인하실 수 있습니다.

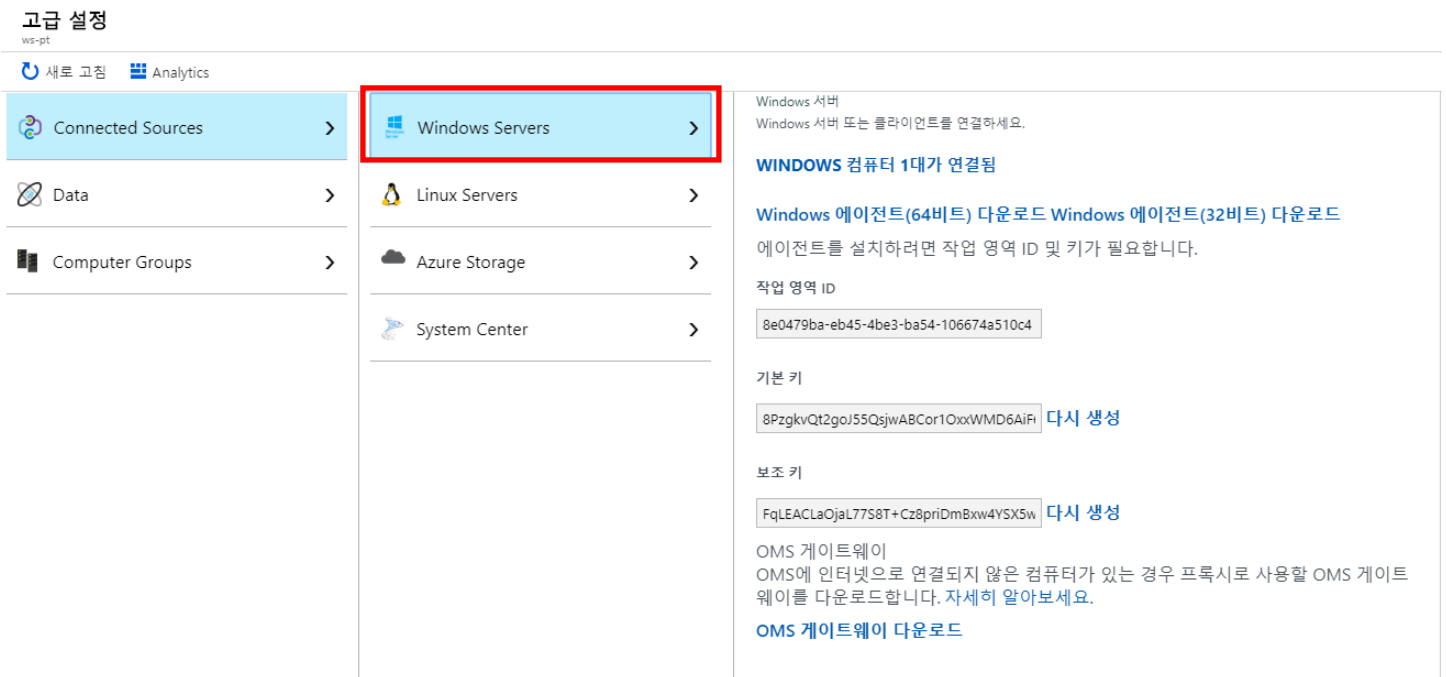


2. Log Analytics 는 oms agent 를 이용하여 데이터를 수집합니다. Log Analytics 는 온프레미스, 클라우드 리소스가 Log Analytics 에 연결될 수 있게 agent 및 다운로드 방법을 가이드 하고 있습니다.

Log Analytics 접속 후 “고급 설정” 선택



“고급 설정” 선택 후 -> “Connected Sources” -> “Windows Server” 선택



Windows 서버

Windows 서버 또는 클라이언트를 연결하세요.

WINDOWS 컴퓨터 1대가 연결됨

Windows 에이전트(64비트) 다운로드 Windows 에이전트(32비트) 다운로드

에이전트를 설치하려면 작업 영역 ID 및 키가 필요합니다.

작업 영역 ID

8e0479ba-eb45-4be3-ba54-106674a510c4

기본 키

8PzgkvQt2goJ55QsjwABCor1OxxWMD6AiFi [다시 생성](#)

보조 키

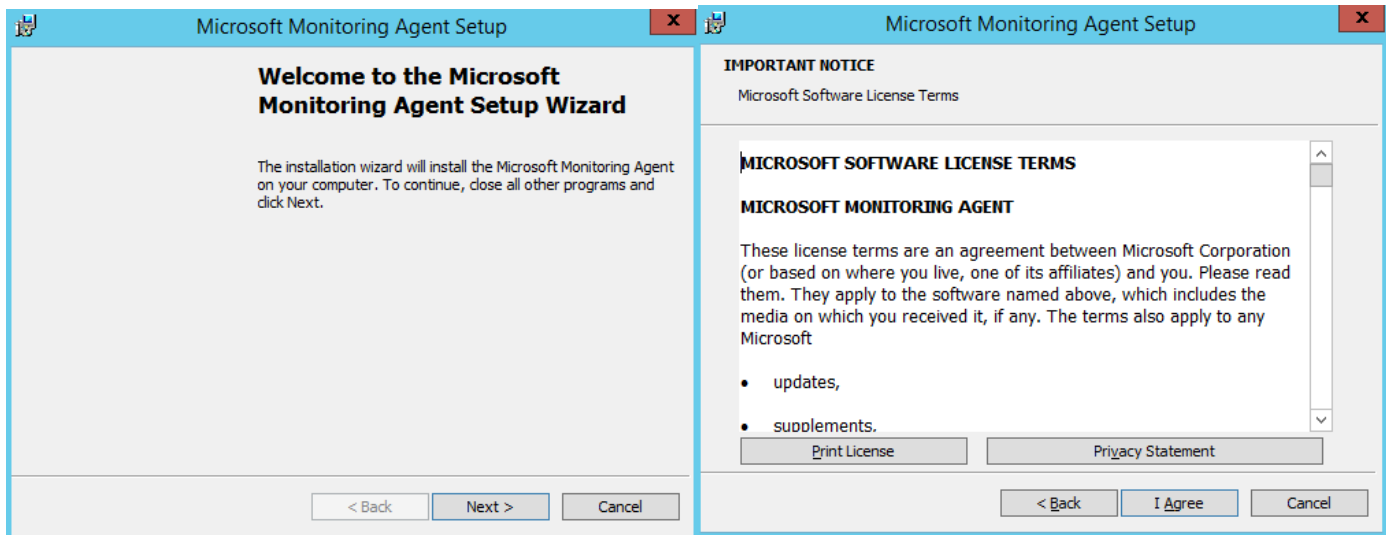
FqLEACLaQjaL77S8T+Cz8priDmBxw4YSX5w [다시 생성](#)

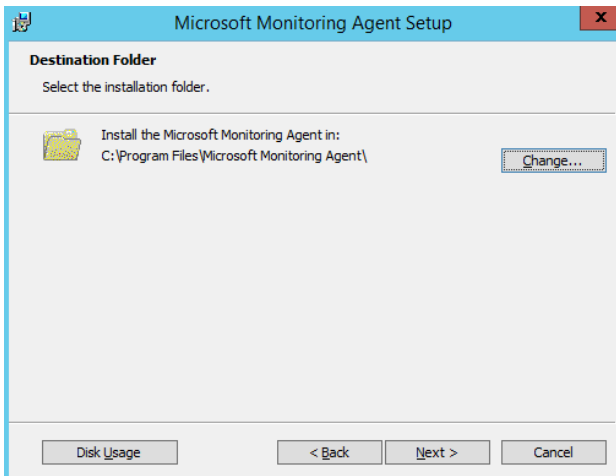
OMS 게이트웨이

OMS에 인터넷으로 연결되지 않은 컴퓨터가 있는 경우 프록시로 사용할 OMS 게이트웨이를 다운로드합니다. [자세히 알아보세요.](#)

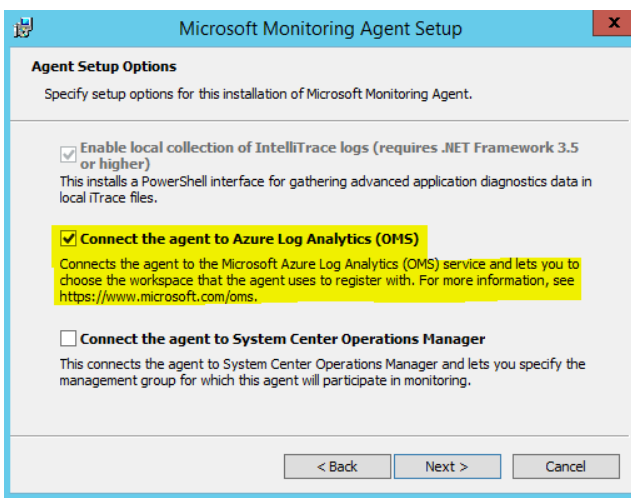
OMS 게이트웨이 다운로드

원하는 디렉토리에 넣고 설치를 진행합니다.

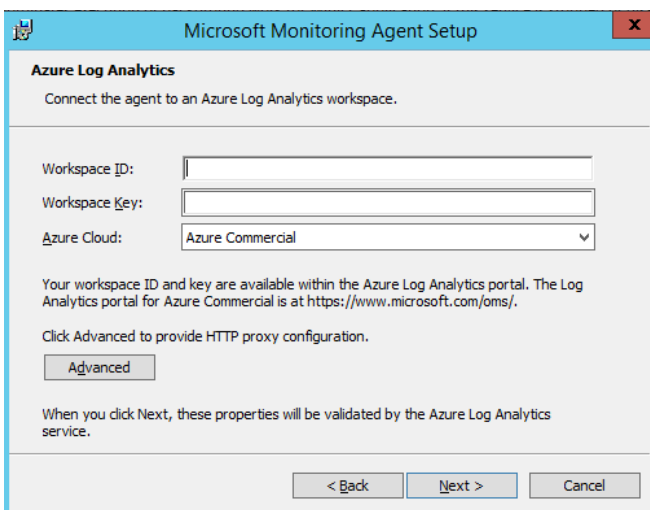




Agent Setup Option 이 나왔을 시 “Connect the agent to Azure Log Analytics(OMS)” 을 선택합니다.



해당 화면이 나왔을때 연결을 위해 Workspace ID, Workspace Key 를 입력합니다.



Log Analytics -> 고급 설정 -> Coonected Source 에서 확인합니다.

Windows Servers >

Linux Servers >

Azure Storage >

System Center >

Windows 서버
Windows 서버 또는 클라이언트를 연결하세요.

WINDOWS 컴퓨터 1대가 연결됨

Windows 에이전트(64비트) 다운로드 Windows 에이전트(32비트) 다운로드
에이전트를 설치하려면 작업 영역 ID 및 키가 필요합니다.

작업 영역 ID
8e0479ba-eb45-4be3-ba54-106674a510c4

기본 키
8PzgkvQt2goJ55QsjwABCor1OxxWMD6AiFi [다시 생성](#)

보조 키
FqLEACLaOjaL77S8T+Cz8priDmBxw4YSX5w [다시 생성](#)

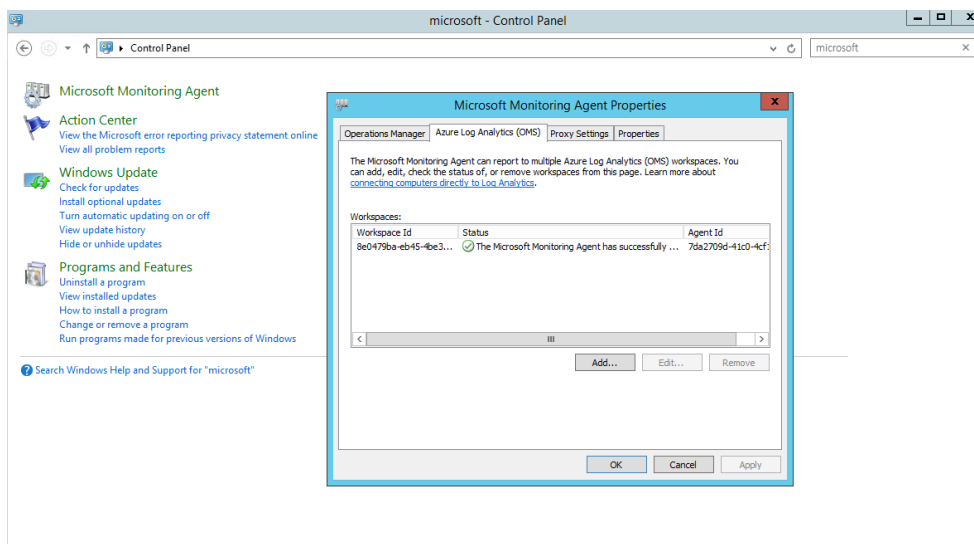
OMS 게이트웨이
OMS에 인터넷으로 연결되지 않은 컴퓨터가 있는 경우 프록시로 사용할 OMS 게이트웨이를 다운로드합니다. [자세히 알아보세요.](#)

[OMS 게이트웨이 다운로드](#)

해당 부분을 넣고 설치를 완료합니다.

제어판에 들어가 해당 연결을 확인합니다.

“Control Panel” -> “Microsoft Monitoring Agent” -> Azure Log Analytics(OMS)



확인 후 Azure Portal 에 들어가 Log Analytics 에 들어가 해당 가상 머신의 “연결” 버튼을 누릅니다.

WS-PT - 가상 컴퓨터

Log Analytics

검색(CTRL+F)

고급 설정

일반

빠른 시작

작업 영역 요약

뷰 디자이너

로그

로그(클래식)

솔루션

가격 책정 계층

사용량 및 예상 비용

속성

저장된 검색

업그레이드 요약

경고

서비스 맵

작업 영역 데이터 원본

가상 컴퓨터

저장소 계정 로그

Azure 활동 로그

범위 구성(미리 보기)

Azure 리소스

새로 고침 ? 도움말

이름으로 필터링...

8개 선택됨

2개 선택됨

이름	OMS 연결	OS
GenVM1	다른 작업 영역	Windows
GenVM2	다른 작업 영역	Linux
GenVM3	다른 작업 영역	Linux
miniflux	연결되지 않음	Linux
minitest-vm	연결되지 않음	Windows
MonitorVM1	다른 작업 영역	Windows
MSFT-HKG-VM01	다른 작업 영역	Windows
PT-MGT-MSM01	연결되지 않음	Windows
PT-PRD-LX01	이 작업 영역	Linux
PT-PRD-LX02	연결되지 않음	Linux
PT-PRD-WN01	이 작업 영역	Windows
PT-PRD-WN02	연결되지 않음	Windows
pt-test-vm01	다른 작업 영역	Windows
SQLVM1	다른 작업 영역	Windows
Srv-IIS01	다른 작업 영역	Windows
Srv-IIS02	다른 작업 영역	Windows
Srv-Jump	다른 작업 영역	Windows
Srv-Work	다른 작업 영역	Windows

PT-PRD-WN02

가상 컴퓨터

연결

연결 끊기

새로 고침

연결 중...

상태

연결 중

작업 영역 이름

WS-PT

메시지

Log Analytics에 VM을 연결하는 중입니다. 상태 업데이트는 나중에 다시 확인하세요.

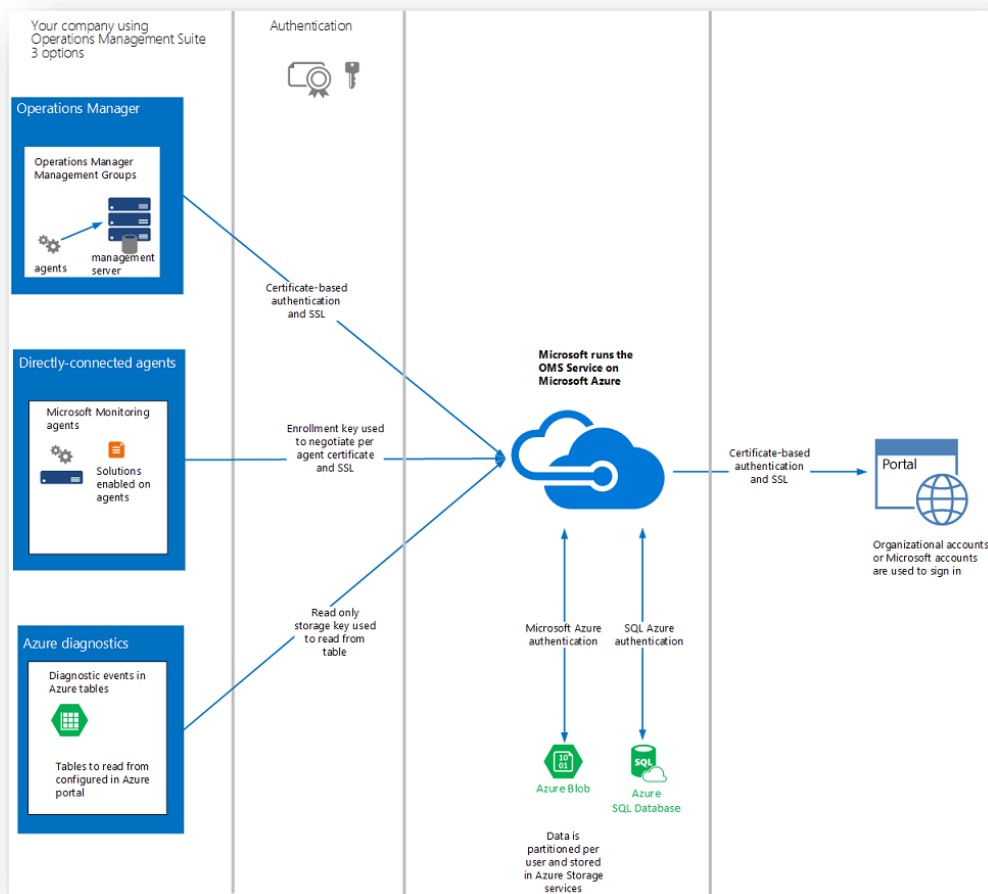
Lab 2. Azure 로그 분석(Log Analytics) 사용하기

실제 구성을 끝내고 "OMS 포털"을 이용하여 Log Analytics 를 사용하는 방법에 대해 간단히 알아봅니다.

"Log Analytics"란 인프라 및 응용프로그램의 로그를 실시간으로 수집, 집계하여 운영을 위한 Insight 를 제공하는 서비스입니다. On-Premise 또는 퍼블릭 클라우드(Microsoft Azure, AWS)에 상관없이 사용이 가능합니다.

• 특징점

- 클라우드 서비스(SaaS) 형태로 제공되기 때문에 초기 환경 구성 및 서비스 관리의 부담이 없으며 항상 최신 버전의 솔루션을 활용할 수 있습니다.
- 하나의 서비스에서 통합하여 기존 on-premise 인프라와 클라우드에 구성된 인프라를 한 화면에서 관리할 수 있습니다.
- 로그 수집을 위한 저장소 관리 및 데이터 관리 노력을 최소화 할 수 있습니다.
- 수십만 로그를 빠르게 분석할 수 있고 권장 사항과 구체적인 정보를 Microsoft Knowledge Data 를 기본으로 제공합니다.
- Windows 와 Linux 모두 OS 수준의 관리가 가능하고 (10 초 주기) 성능 수집 및 분석이 가능합니다.



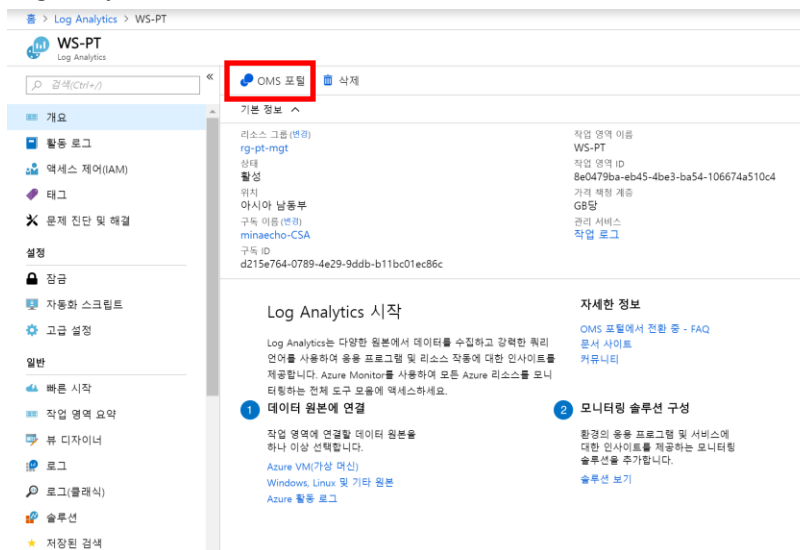
"Log Analytics" 는 솔루션 갤러리 기반으로 서비스를 제공합니다.

크게 4 가지 솔루션으로 나뉘어져있습니다 (Insight & Analytics, Automation & Control, Security & Compliance, Protection & Recovery)



1. Azure Portal 에 접속하여 "Log Analytics" 선택 후

Log analytics -> OMS 포털 선택

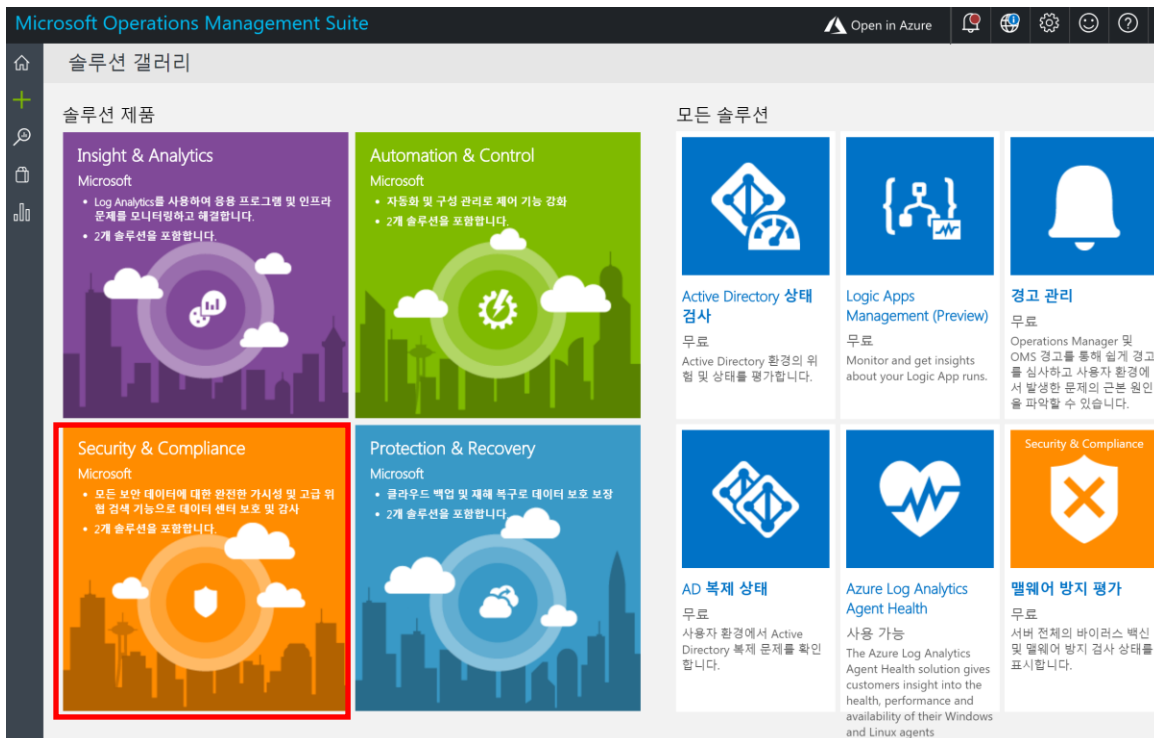


2. OMS 포탈 화면 -> "솔루션 갤러리" 선택



각각의 솔루션을 선택하면 솔루션에 대한 설명과 사용할 서비스 목록이 나타납니다.

"Security & Compliance" 선택



다음과 같은 화면이 나타나고 완료되면 자동으로 서비스가 대시보드에 추가됩니다.

Security & Compliance

☼ 솔루션 추가 중...

포함된 솔루션:

- 맬웨어 방지 평가
- 보안 및 감사

Antimalware Assessment

데이터에 연결하는 중

Microsoft Operations Management Suite에서 처음으로 맬웨어 평가를 수행하기 위해 서버 데이터에 연결하고 있습니다. 이 작업에는 몇 시간 정도 소요됩니다.

Security and Audit

평가 수행 중

Microsoft Operations Management Suite가 처음으로 보안 평가를 수행하기 위해 서버 데이터에 연결되고 있습니다. 이 작업은 몇 시간이 걸립니다. 따라서 야간에 실행하는 것이 좋습니다.

서버 데이터를 연결하는 데에는 시간이 소요됩니다. 따라서 OMS Setting 을 진행하실때는 야간에 실행하는 것을 추천드립니다. 해당 부분은 시나리오 2 에서 실습해볼 수 있습니다.

3. OMS Agent 를 통해 저장되는 로그를 쿼리하는 방법에 대해 알아봅니다.

OMS Portal 에 들어가 “로그 검색”을 선택합니다.

Microsoft Operations Management Suite

로그 검색

☆ 즐겨찾기 ⌚ 내역 📊 분석

실행

고급 분석

Usage | where IsBillable == true | summarize count() by DataType

모든 사용 레코드 반환 결과 파일형 청구 가능한 레코드 필터링 결과 파일형 DataType별 레코드 수 계산

시도해 볼 쿼리가 몇 가지 더 있습니다.

수집된 모든 데이터

"windows"를 포함하는 하트비트 레코드 검색

매시간 하트비트를 보낸 고유 컴퓨터의 수 계산

각 호스트 이름 및 기능 조합에 대해 수집된 syslog 레코드 수 계산
필수 데이터 수집: Syslog

매시간 각 인스턴스에 대해 보고된 평균 사용 가능한 메모리를 차트로 작성
필수 데이터 수집: 성능 카운터

시작

- 5분 내 램프 업(ramp-up) 쿼리 언어 참고 자료
- 문제 해결을 위한 도움말을 보려면 쿼리 시작 새 쿼리 작성 방법을 알아보려면
- 참조하세요. 쿼리 언어 참조 함수, 연산자 및 형식에 대한 자세한 내용은
- 문자열 작업에 관한 자습서를 확인한 다음에 날짜 및 시간 작업을 확인하여 데이터 형식에 대해 자세히 알아보려면
- 사용 집계 데이터에 대한 인사이트 열기

아래에 시도해볼 수 있는 쿼리들이 예시로 나와있습니다.

시나리오 1. OMS 에 정상적인 하트비트를 보낸 고유 컴퓨터 수 확인

1. 테스트를 위해 “매시간 하트비트를 보낸 고유 컴퓨터의 수 계산”을 선택합니다.

Microsoft Operations Management Suite

로그 검색

☆ 즐겨찾기 ⌚ 내역 📊 분석

실행

고급 분석

Usage | where IsBillable == true | summarize count() by DataType

모든 사용 레코드 반환 결과 파일형 청구 가능한 레코드 필터링 결과 파일형 DataType별 레코드 수 계산

시도해 볼 쿼리가 몇 가지 더 있습니다.

수집된 모든 데이터

"windows"를 포함하는 하트비트 레코드 검색

매시간 하트비트를 보낸 고유 컴퓨터의 수 계산

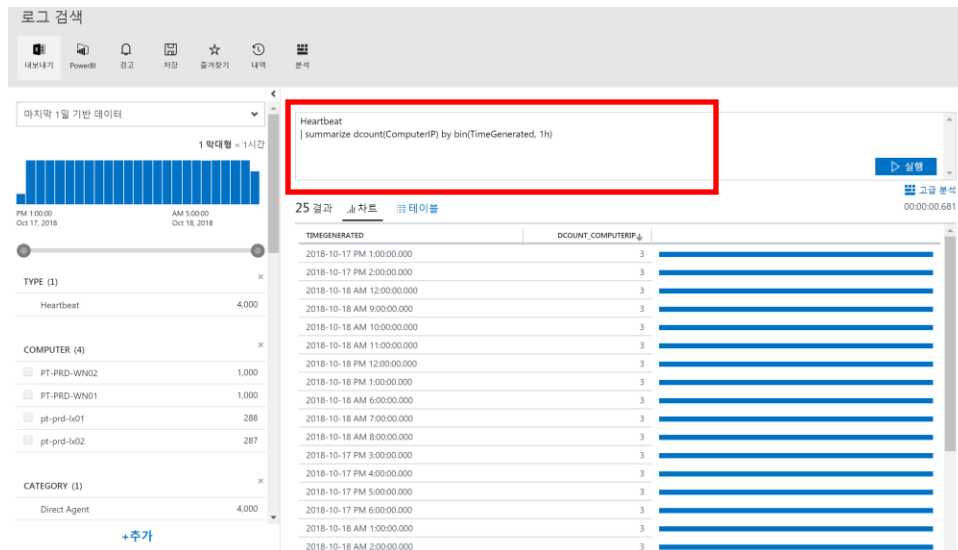
각 호스트 이름 및 기능 조합에 대해 수집된 syslog 레코드 수 계산
필수 데이터 수집: Syslog

매시간 각 인스턴스에 대해 보고된 평균 사용 가능한 메모리를 차트로 작성
필수 데이터 수집: 성능 카운터

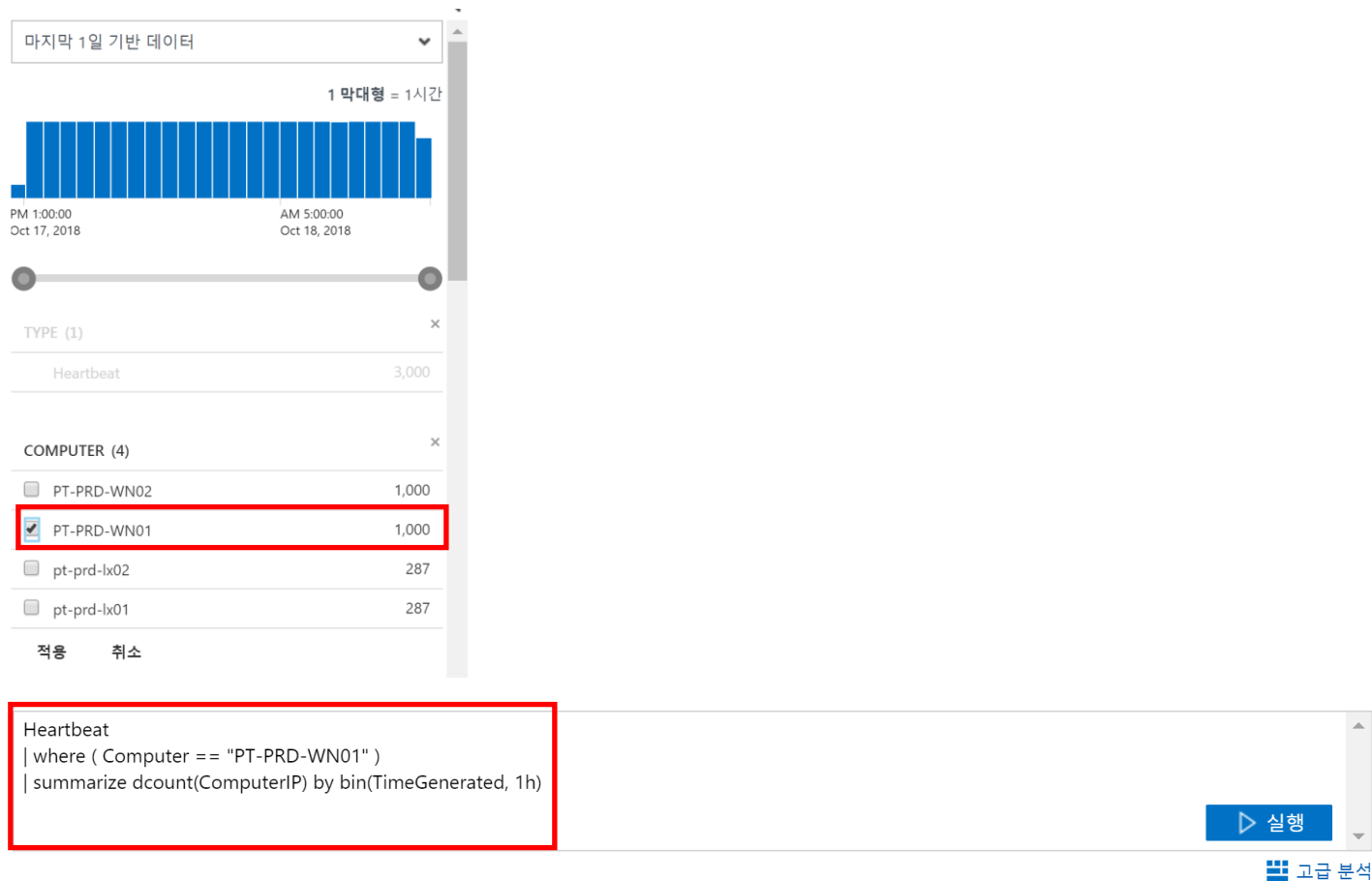
시작

- 5분 내 램프 업(ramp-up) 쿼리 언어 참고 자료
- 문제 해결을 위한 도움말을 보려면 쿼리 시작 새 쿼리 작성 방법을 알아보려면
- 참조하세요. 쿼리 언어 참조 함수, 연산자 및 형식에 대한 자세한 내용은
- 문자열 작업에 관한 자습서를 확인한 다음에 날짜 및 시간 작업을 확인하여 데이터 형식에 대해 자세히 알아보려면
- 사용 집계 데이터에 대한 인사이트 열기

선택을 하게 되면 기본적인 쿼리와 결과 화면이 나타나게 됩니다.



2. 왼쪽에 있는 항목들을 선택하게 되면 관련 쿼리가 구체적으로 구성되게 됩니다.

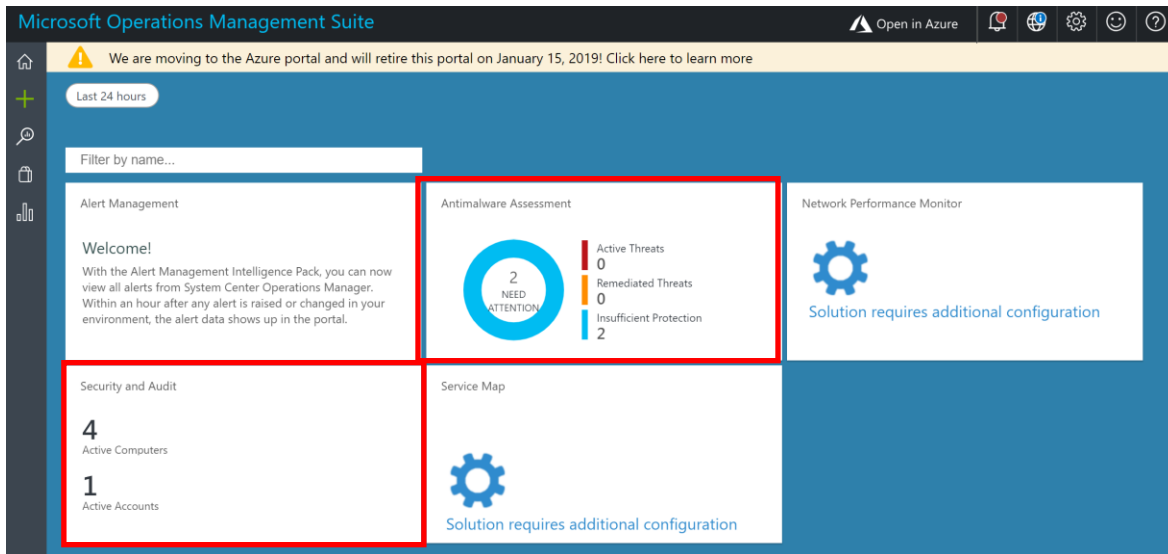


시나리오 2. 갤러리를 이용한 결과 확인 및 쿼리 확인

OMS 는 솔루션 갤러리를 기반으로 서비스를 사용할 수 있습니다. 현재 Security & Compliance 솔루션이 설치되어 있는 상태입니다. (17-19 page 참고) 솔루션이 제공하는 기능과 관련하여 쿼리를 사용하는 방법에 대해 알아봅니다.

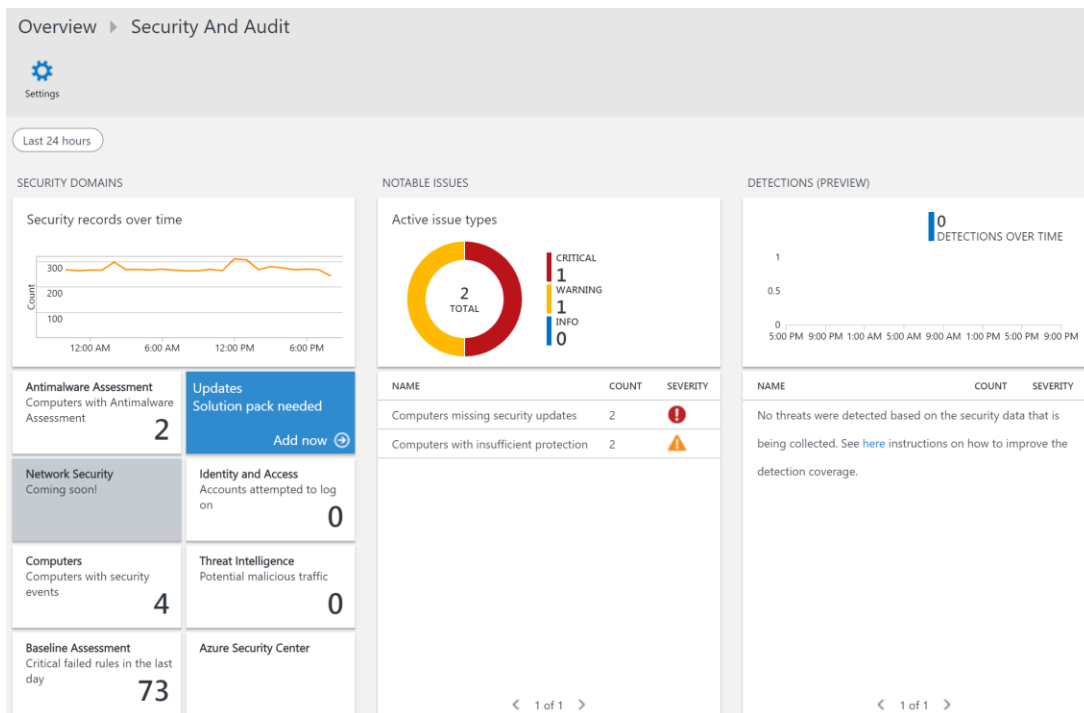
1. OMS Portal 대시보드 화면을 보면 Security & Compliance 솔루션이 활성화 된것을 확인할 수 있습니다.

(Security and Audit, Antimalware Assessment)



2. Security and Audit 을 선택합니다.

보안에 관련하여 전반적인 내용이 대시보드에 나타나고 있으며 선택하면 더 자세한 내용을 볼 수 있습니다.



3. "Notable Issues"에서 "Severity"가 Critical 한 항목을 선택해 해당 내용을 확인합니다.

NOTABLE ISSUES

Active issue types

NAME	COUNT	SEVERITY
Computers missing security updates	2	CRITICAL
Computers with insufficient protection	2	WARNING

Log Search

Export PowerBI Alert Save Favorites History Analytics

Data based on last 1 day

1 bar = 1hr

Update

| where UpdateState == 'Needed' and Optional == false and Classification == 'Security Updates' and Approved != false | summarize count() by Computer

RUN

2 Results

COMPUTER	COUNT
PT-PRD-WN01	4
PT-PRD-WN02	4

4 Results

List Table **Computer Security**

Advanced Analytics 00:00:00.292

Selected computer

PT-PRD-WN01

Notable issue

Computers missing security updates- These computers do not have the latest security updates installed. There are many attacks that are exploiting known vulnerabilities that were already fixed, therefore it is strongly recommended to always have your computers up to date.

Operation system

Microsoft Windows Server 2012 R2 Datacenter

Antimalware protection status

Not reporting

Antimalware threats status

Unknown

Malicious IPs

0

Security events

EVENT	COUNT
4688 - A new process has been...	2K
5059 - Key migration operation.	48
4624 - An account was successf...	3
4672 - Special privileges assign...	3

See all...

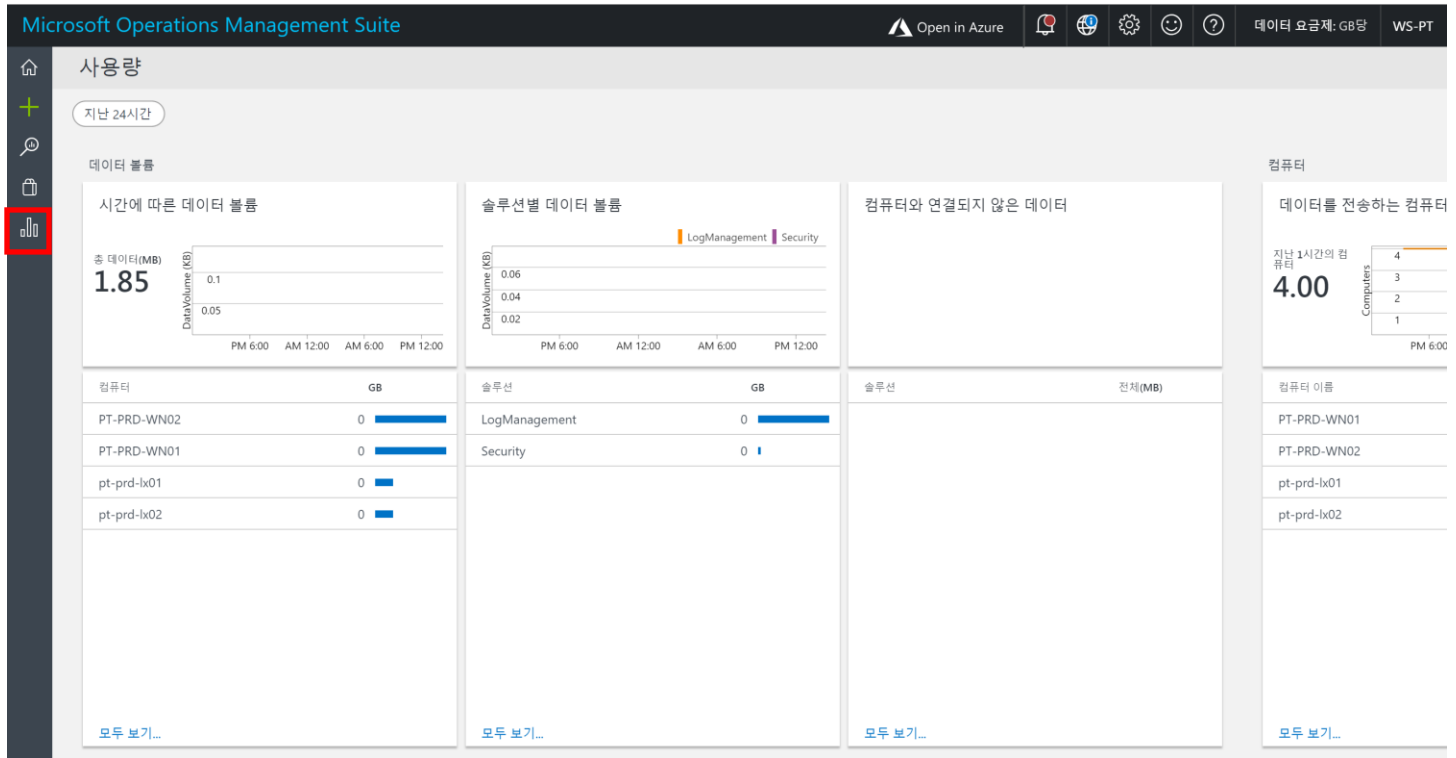
Accounts logged on

ACCOUNT	COUNT
No account logged on	

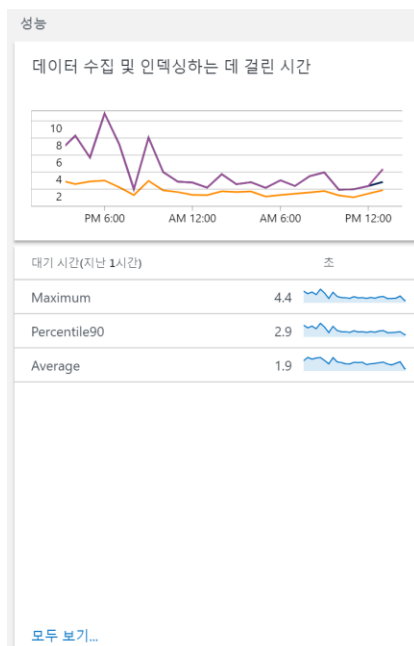
See all...

OMS 는 OMS 사용에 대한 로그를 제공합니다.

“OMS Portal” -> “사용량” 선택



데이터 볼륨, 컴퓨터, 제공, 성능, 쿼리 목록에 대한 사용량을 제공하고 있습니다.



Lab 3. Azure 보안 센터(Security Center) 사용하기

Azure Security Center 는 하이브리드 클라우드 워크로드에 통한 보안 관리 및 고급 위협 방지를 제공하고 있습니다.

보안 센터(Security Center)를 사용하여 워크로드에 대한 보안 정책 적용, 외부 공격에 대한 검색 및 대응이 가능합니다.

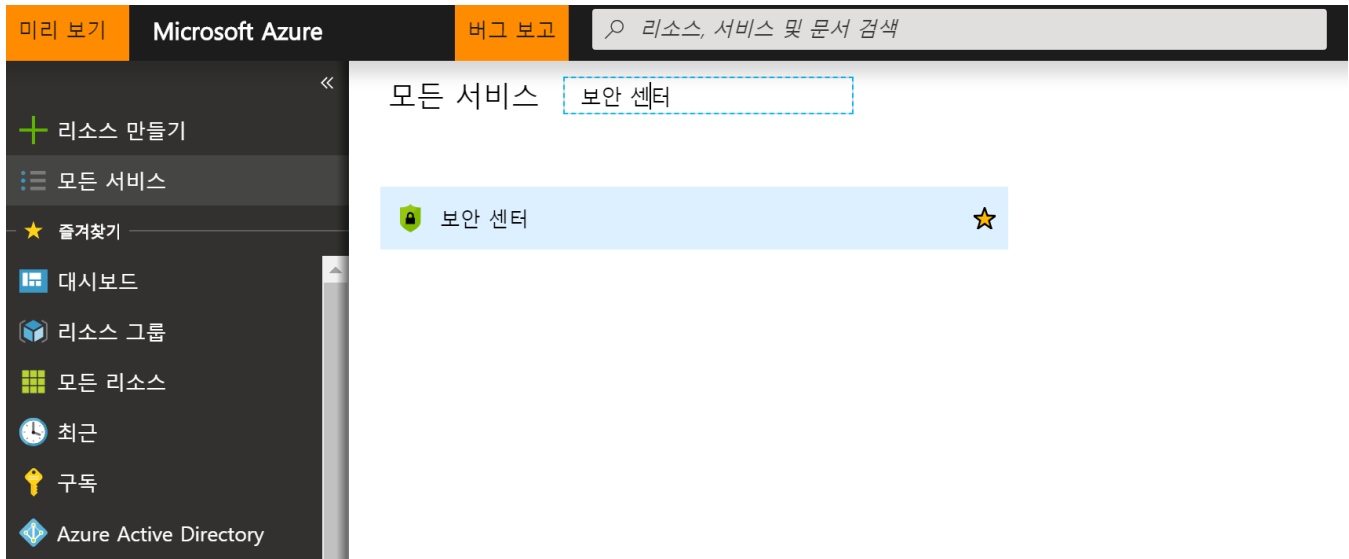
보안센터 특징점

- 중앙 집중식 정책 관리 – 모든 하이브리드 클라우드 작업에 걸쳐 보안 정책을 중앙에서 관리하여 회사 또는 규정 보안 요구 사항을 준수할 수 있습니다.
- 연속 보안 평가 – 가상 머신, 네트워크, 저장소 및 데이터 서비스, 응용 프로그램의 보안 상태를 모니터링하여 잠재적인 보안 문제를 찾아낼 수 있습니다.
- 실행 가능 권장 지침 – 우선 순위가 지정된 보안 권장 지침을 사용하여 공격자들이 악용하기 전에 보안 취약성을 수정할 수 있습니다.
- 경고 및 인시던트 우선 순위 지정 – 우선 순위가 지정된 보안 경고와 인시던트를 통해 가장 중요한 위협부터 중점적으로 확인할 수 있습니다.
- 고급 클라우드 방어 – 관리 포트 및 적응형 응용 프로그램 제어에 대한 Just-In-Time 액세스를 통해 가상머신에서 실행되는 응용 프로그램을 제어함으로써 위협을 줄일 수 있습니다.
- 통합 보안 솔루션 – 연결된 파트너 솔루션을 포함한 여러 소스에서 보안 데이터를 수집, 검색 및 분석할 수 있습니다.

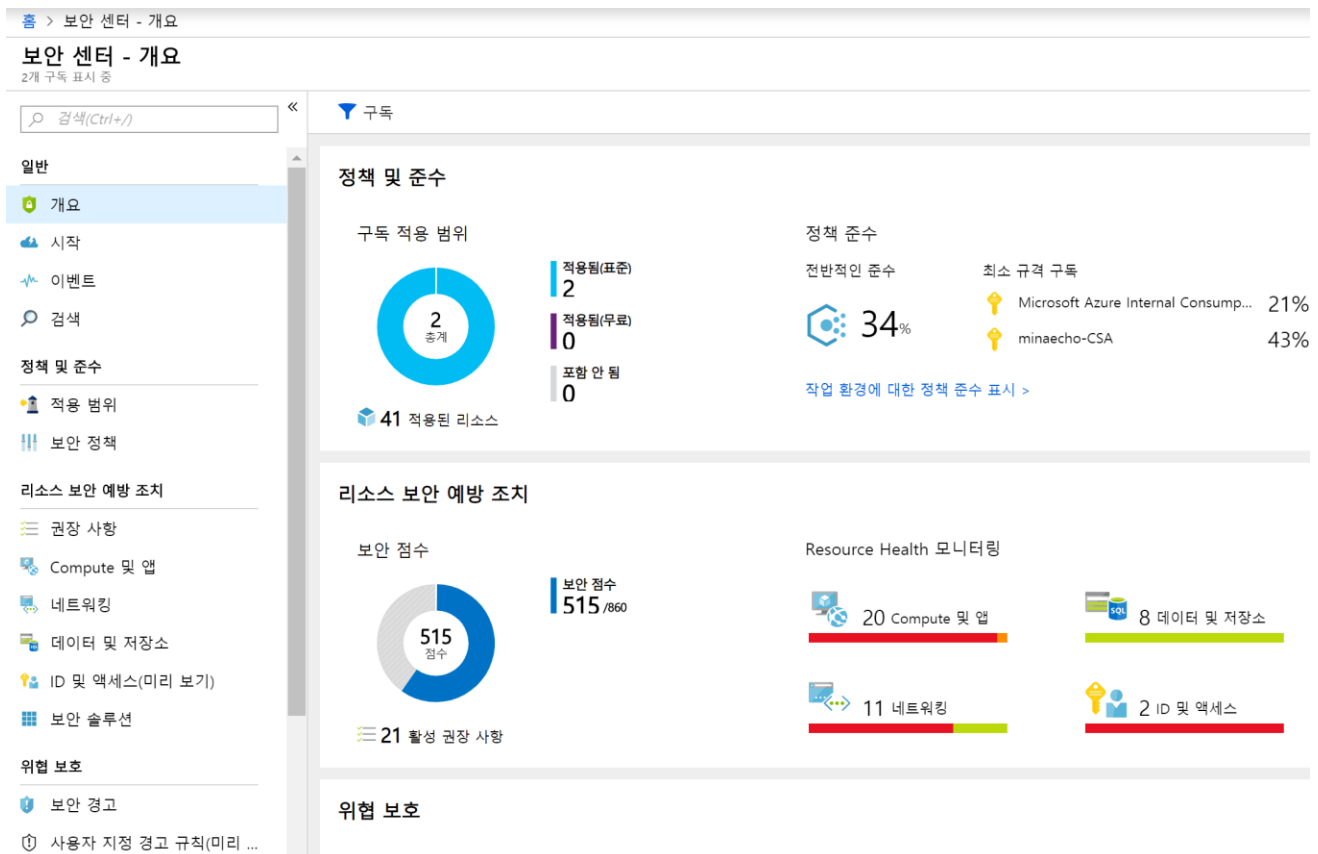


1. Azure 보안 센터 설정하기

Azure Portal 에서 "모든 서비스" 선택 후 "보안 센터"를 검색합니다.



보안 센터의 화면은 다음과 같이 구성되어 있습니다.



보안 센터를 사용하려면 먼저 적용 범위와, 보안 정책을 설정하여야 합니다.

적용 범위는 무료와 표준 계층으로 나뉘어져 있습니다. 무료와 표준은 지원하는 범위가 조금 다르며 표준 계층의 경우 처음 60 일간 무료로 제공됩니다. 60 일을 초과하면 사용량 기반으로 요금이 과금됩니다.

금액에 관련된 부분은 해당 url 을 참고해주세요.(<https://azure.microsoft.com/ko-kr/pricing/details/security-center/>)

현재 시나리오는 “표준 계층” 을 사용합니다.

기능	무료 계층	표준 계층
보안 정책, 평가 및 권장 사항	✓	✓
연결된 파트너 솔루션	✓	✓
보안 이벤트 컬렉션 및 검색	--	✓
JIT(Just In Time) VM 액세스	--	✓
적응 응용 프로그램 제어	--	✓
고급 위협 감지	--	✓
기본 제공 및 사용자 지정 경고	--	✓
위협 인텔리전스	--	✓

2. 적용 범위, 보안 정책 설정

“정책 및 준수” 에 들어가 구독 또는 관리 그룹에 대한 보안 정책을 관리합니다.

“보안 센터” -> “적용 범위” -> “표준 적용 범위”

홈 > 보안 센터 - 적용 범위

보안 센터 - 적용 범위

2개 구독 표시 중

일반

- 개요
- 시작
- 이벤트
- 검색
- 정책 및 준수
- 적용 범위**
- 보안 정책

포함 안 됨 기본 적용 범위 **표준 적용 범위**

좋습니다. 아래 구독은 완전히 보호됩니다.

2 구독

구독 검색

이름	내 역할	소유자	리소스
minaecho-CSA	Owner	소유자 표시	23
Microsoft Azure Inte...	Owner	소유자 표시	18

보안 센터 - 보안 정책

2개 구독 표시 중

검색(CTRL+/)

일반

- 개요
- 시작
- 이벤트
- 검색

정책 및 준수

- 적용 범위
- 보안 정책**
- 리소스 보안 예방 조치
- 권장 사항
- Compute 및 앱
- 네트워킹
- 데이터 및 저장소
- ID 및 액세스(미리 보기)

정책 관리

아래 목록에서 구독 또는 관리 그룹을 선택하여 보안 정책을 관리합니다. 추가 정책을 정의하기 위해 예외 및 고급 설정을 관리합니다.
[자세한 내용을 보려면 여기를 클릭 >](#)

5 관리 그룹 2 구독 2 작업 영역

이름으로 검색

이름	정책 이니셔티브 할당	호환	적용 범위	설정
Microsoft Azure Internal Consumption		21%	표준	설정 편집 >
minaecho-CSA		43%	표준	설정 편집 >
72f988bf-86f1-41af-91ab-2d7cd011db47(0/5개...)	제한된 권한		---	설정 편집 >
WS-PT	---	---	---	설정 편집 >
SC-LA	---	---	---	설정 편집 >

"보안 정책" -> "데이터 수집" -> Windows 보안 이벤트

"일반" -> "저장"

보안 정책 - 데이터 수집

ws-pt

검색(CTRL+/)

정책 구성 요소

- 가격 책정 계층
- 데이터 수집**

저장

추가 원시 데이터 저장

Log Analytics 작업 영역에 원시 이벤트, 로그 및 추가 보안 데이터를 저장할 수 있습니다. 이 데이터를 사용하면 위협의 감사, 조사 및 분석을 수행할 수 있습니다.

Windows 보안 이벤트

수집하고 저장할 Windows 보안 이벤트를 선택합니다. 선택을 없음에서 다른 항목으로 변경하면 저장된 이벤트에 대한 요금 부과가 시작됩니다.
[추가 정보](#)

☐ 모든 이벤트
모든 Windows 보안 및 AppLocker 이벤트입니다.

☒ 일반
감사 용도의 표준 이벤트 집합입니다.

☐ 최소
잠재적인 위협을 나타낼 수 있는 작은 이벤트 집합입니다. 이 옵션을 사용하도록 설정하면 전체 감사 내역을 포함할 수 없습니다.

☐ 없음
보안 또는 AppLocker 이벤트가 없습니다.

3. Azure Security Center 기능 알아보기

Azure Security Center 가 제공하는 기능에 대해 알아봅니다.

시나리오 1. 리소스 보안 예방 조치

“보안 센터” -> “리소스 보안 예방 조치” -> “Compute 및 앱” -> 확인할 가상 머신 선택 (“PT-PRD-WN01”)

보안 센터 - Compute 및 앱

2개 구독 표시 중

검색(Ctrl+F)

리소스 보안 예방 조치

권장 사항

Compute 및 앱

네트워킹

데이터 및 저장소

ID 및 액세스(미리 보기)

보안 솔루션

위협 보호

보안 경고

사용자 지정 경고 규칙(미리 보...

보안 경고 맵(미리 보기)

자동화 및 오케스트레이션

플레이북(미리 보기)

PT-PRD-WN01

보안 상태

Resource health

PT-PRD-WN01

총 추천 4

상태별 권장 사항

상태	개수
높음	2
중간	1
낮음	1

information

리소스 이름 PT-PRD-WN01

리소스 그룹 RG-PT-DEMO

구독 minaecho-CSA

버전 계산

작업 영역 ws-pt

모니터링 상태 Azure 보안 센터에서 모니터링

운영 체제 Windows

시스템 업데이트 Microsoft (마지막 검사 시간 - 최근 데 이터 없음)

보안 구성 Microsoft (마지막 검사 시간 - 최근 데 이터 없음)

Recommendation list

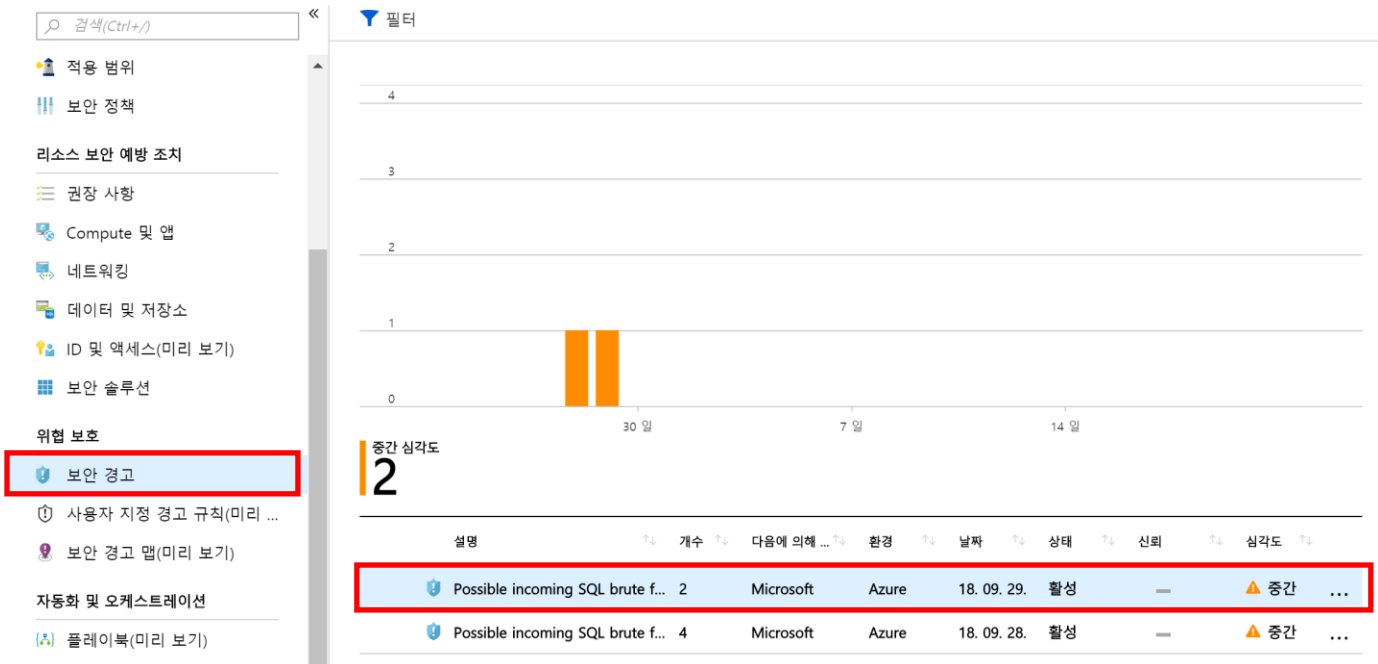
권장 사항 통과된 평가(2개) 사용할 수 없는 평가(6개)

설명	상태
Install endpoint protection solution on virtual machines	높음
Apply disk encryption on your virtual machines	높음
Install a vulnerability assessment solution on your virtual machines	중간
Troubleshoot missing scan data on your machines	낮음

시나리오 2. 위협 보호

Azure Security Center 는 외부에서부터 오는 위협을 감지 및 보호합니다. 또한 기계 학습을 사용하여 패턴을 분석하여 보안에 대한 경고를 줍니다.

“위협 보호” -> “보안 경고”



눌러보면 공격 받은 리소스와 관련 상세 정보를 알 수 있습니다.

Possible incoming SQL brute force attempts detected

필터

공격받은 리소스	개수	검색 시간	환경	상태	신뢰	심각도
sqlvm1	1	오전 9:00:00	Azure	활성	—	중간
sqlvm1	1	오전 3:00:00	Azure	활성	—	중간

Possible incoming SQL brute force attempts detected

자세한 정보

일반 정보

설명	Network traffic analysis detected incoming SQL communication to 52.231.10.108, associated with your resource sqlvm1, from 211.35.149.151. Specifically, sampled network data shows suspicious activity between 9/28/2018 12:07:52 AM UTC and 9/28/2018 10:44:26 PM UTC on port 1433 (Microsoft SQL Server). This activity is consistent with brute force attempts against SQL servers.
검색 시간	2018년 9월 29일 토요일 오전 9:00:00
심각도	중간
상태	활성
공격받은 리소스	sqlvm1
구독	Microsoft Azure Internal Consumption (7dc7f264-cd4b-4507-b2b9-4b82a877920f)
다음에 의해 검색됨	Microsoft
수행한 작업	검색됨
환경	Azure
리소스 종류	Virtual Machine