

클라우드 개념 설명

실습경로 : <https://www.notion.so/Azure-9ad187bcdeeb4c639eb3266622398c23>

CapEX(자본지출) / OpEx(운영지출)

- 과거에는 초기 인프라를 구성을하거나 작동 중 추가적인 리소스에 대한 상당한 요금이 발생하였다
 - 클라우드 컴퓨팅 서비스의 등장으로 초기비용이나 장비의 설치 시간 없이 고객에게 컴퓨팅 서비스를 제공할 수 있다
1. **CapEX**
물리적 인프라에 대한 비용을 초기에 지출한 다음, 시간이 지남에 따라 납입 고지서에서 비용을 공제하는 것이다
(일반적인 온프레미스 환경의 지출방식)
 2. **OpEX**
초기에 비용이 발생하지 않고, 현재 서비스 또는 제품에 대해 지출되어 청구되고 있는 비용이다.
(일반적인 클라우드 환경의 지출방식)

클라우드 서비스 특징

1. Fault Tolerance(결함 감내 시스템)

: 시스템을 구성하는 부품의 일부에서 결함 또는 고장이 발생하여도 정상적 혹은 부분적으로 기능을 수행 할 수 있는 시스템, 치명적인 결함이나 고장이 발생하면 시스템 정지

2. Disaster Recovery(재해 복구)

: 자연재해나 인위적인 재해가 일어나면 특정 단체에 중요한 기술 인프라를 복구하거나 지속할 목적으로 준비하는 과정, 정책, 절차를 의미

3. Dynamic scalability(확장성)

: 클라우드에서 workload가 증가할 시 부하를 감당할 수 있을 만한 Resource Capacity를 갖고 있느냐에 대한 능력

4. Elasticity(탄력성)

: 막대양 양의 resource 용량에 대해서 순간적으로 할당하거나 해제하는 능력에 대한 성질
즉, 요구에 걸맞는 resource를 얼마나 빠르고 효과적으로 할당하는지에 대한 능력

5. Low Latency(짧은 지연시간)

: 인터넷에 빠르게 액세스 할 수 있는 클라우드 서비스

클라우드 배포 모델

- 클라우드 배포 모델은 데이터가 저장되는 위치, 고객이 어떻게 가져오고, 어디에서 애플리케이션을 실행하는지에 대한 것에 따라 분류된다
1. **퍼블릭 클라우드**
 - 가장 일반적인 배포 모델로, 관리하거나 최신 상태로 유지할 로컬 하드웨어가 없다
 - 모든 항목이 클라우드 공급자의 하드웨어에서 실행된다
 - 경우에 따라 다른 클라우드 사용자와 컴퓨팅 리소스를 공유하여 비용을 추가로 절감 할 수 있다(여러 기업이 각각 클라우드에서 리소스의 일부를 사용하는 공용 엔티티)
 2. **프라이빗 클라우드**
 - 사용자 고유의 데이터 센터에 클라우드 환경을 만들고, 컴퓨팅 리소스에 대한 셀프 서비스 액세스를 조직의 사용자에게 공급한다
 - 제공하는 하드웨어 및 소프트웨어 서비스의 구매 및 유지 관리에 대한 전적인 책임을 가진다
 3. **하이브리드 클라우드**
 - 퍼블릭 및 프라이빗 클라우드를 결합하므로 가장 적합한 위치에서 애플리케이션을 실행 할 수 있는 배포 모델
 - 웹 사이트를 퍼블릭 클라우드에서 호스팅하고, 데이터베이스와 같은 서비스는 프라이빗 클라우드에 호스팅하여 안전하게 연결 할 수 있다

클라우드 서비스 형식

| | IaaS | PaaS | SaaS |
|--------------|---|---|--|
| 초기 비용 | 초기 비용이 없습니다. 사용자는 사용하는 항목에 대해서만 지불합니다. | 초기 비용이 없습니다. 사용자는 사용하는 항목에 대해서만 지불합니다. | 사용자가 부담하는 초기 비용이 없으며, 일반적으로 구독에 대한 월간 또는 연간 기준의 요금을 지불합니다. |
| 사용자 소유권 | 사용자는 자신의 소프트웨어 운영 체제, 미들웨어 및 애플리케이션을 구입, 설치, 구성 및 관리해야 합니다. | 사용자는 자신의 애플리케이션을 개발해야 하지만, 서버 또는 인프라를 관리할 필요가 없습니다. 이를 통해 사용자는 실행 하려는 애플리케이션 또는 워크로드에만 집중할 수 있습니다. | 사용자는 애플리케이션 소프트웨어만 사용하며, 해당 소프트웨어를 유지하거나 관리할 필요가 없습니다. |
| 클라우드 공급자 소유권 | 클라우드 공급자는 사용자에게 기본 클라우드 인프라(예: 가상 머신, 스토리지 및 네트워킹)를 제공해야 합니다. | 클라우드 공급자는 운영 체제를 관리하고, 네트워크와 서비스를 구성해야 합니다. 클라우드 공급자는 일반적으로 사용자가 실행하려는 애플리케이션 이외의 모든 것을 담당하며, 애플리케이션을 실행할 수 있는 완전 관리형 플랫폼을 제공합니다. | 클라우드 공급자는 애플리케이션 소프트웨어를 프로비전, 관리 및 유지해야 합니다. |

| 온-프레미스 | IaaS (Infrastructure as a Service) | PaaS (Platform as a Service) | SaaS (Software as a Service) |
|--------|---------------------------------------|---------------------------------|---------------------------------|
| 애플리케이션 | 애플리케이션 | 애플리케이션 | 애플리케이션 |
| 데이터 | 데이터 | 데이터 | 데이터 |
| 런타임 | 런타임 | 런타임 | 런타임 |
| 미들웨어 | 미들웨어 | 미들웨어 | 미들웨어 |
| OS | OS | OS | OS |
| 가상화 | 가상화 | 가상화 | 가상화 |
| 서버 | 서버 | 서버 | 서버 |
| 스토리지 | 스토리지 | 스토리지 | 스토리지 |
| 네트워킹 | 네트워킹 | 네트워킹 | 네트워킹 |

Azure란?

- Microsoft의 클라우드 컴퓨팅 플랫폼으로, 조직이 현재와 향후 비즈니스 과제를 해결하도록 돕는 지속적으로 확장 중인 일련의 클라우드 서비스이다
- 사용자가 요구하는 도구와 프레임워크를 사용하여 대규모 글로벌 네트워크에서 애플리케이션을 자유롭게 빌드, 관리 및 배포 할 수 있다

Azure 체험계정

- Azure 체험 계정이 있으면 12개월동안 별도 비용없이 이용할 수 있는 여러 Azure 제품에 액세스 할 수 있음
- 가입일로부터 처음 30일 동안 224,930원의 크레딧을 사용할 수 있으며, 항상 무료로 제공되는 25개 이상의 제품에도 액세스 할 수 있음
- 크레딧을 다 쓰거나 30일이 지난 후에는, 사용자가 종량제 계정으로 업그레이드를 해야만 지출 한도가 제거되므로 모든 무료 제품에 액세스 할 수 있음
- 크레딧은 모든 국가에서 사용이 가능하다(US Goverment, Azure 중국 및 Azure 독일 지역의 독립적 클라우드는 제외)
- Marketplace에서는 크레딧이 적용되지 않지만, 대부분의 솔루션이 해당 솔루션에 대한 평가판 및 무료 계층 요금제를 적용
- 평가판 계정이 종료되면 Azure AD의 계정은 생성 할 수 있지만 기존의 VM은 사용하지 못한다

 ₩224,930 크레딧 남음 >

'무료 체험' 구독에 ₩224,930 크레딧이 남아 있습니다.

[종량제 구독으로 업그레이드하려면 여기를 클릭하세요.](#)

6분 전

Azure 지원 폴린

- Azure는 고객에게 사후 및 사전 기술 지원을 제공한다
- 사용자는 요구에 가장 적합한 지원 폴린을 선택하여 Azure 웹사이트 또는 Portal에서 업그레이드가 가능하다

| 기본 | 개발자 | 표준 | 전문가 지원 | |
|-------|--|---|-------------------------------------|-------------------------------------|
| 범위 | Microsoft Azure: 대금 청구 및 구독 지원, 온라인 자가 진단 | Microsoft Azure: 평가판 및 프로덕 션 이외 환경 | Microsoft Azure: 프로덕션 워크로드 환경 | Microsoft Azure: 업무상 중요한 종 속성 |
| 기술 지원 | | 이메일로 지원 엔 지니어에게 업무 시간에 액세스 ¹ | 이메일 및 전화로 지원 엔지니어에게 연중무휴로 액세스 | 이메일 및 전화로 지원 엔지니어에게 연중무휴로 액세스 |

| | | | |
|--------------|--------|--|--|
| 사례 심각도/응답 시간 | | 최소한의 비즈니스 영향(Sev C): <업무 시간 8시간 ¹ | 최소한의 비즈니스 영향(Sev C): <업무 시간 4시간 ¹ |
| 아키텍처 지원 | 일반 지침 | 보통 비즈니스 영향(Sev B): <4시간 | 보통 비즈니스 영향(Sev B): <2시간 |
| 작업 지원 | | 심각한 비즈니스 영향(Sev A): <1시간 | 심각한 비즈니스 영향(Sev A): <1시간 |
| 학습 | | | 모범 사례를 토대로 ProDirect 배달 관리자가 제공하는 아키텍처 관련 안내 |
| 자동 관리 지침 | | | 온보딩 서비스, 서비스 검토, Azure Advisor 상담 |
| 지원 시작 | | | Azure 엔지니어링 주도 웰 세미나 |
| 가격 책정 | \$29/월 | \$100/월 | \$1,000/월 |

국가/지역

- 가까운 곳에 있고 대기시간이 짧은 네트워크를 통해 연결된 데이터 센터를 하나 이상 포함하고 있는 지리적 영역을 의미, 각 지역의 리소스를 지능적으로 할당하고 제어하여 워크로드의 적절한 균형을 유지한다
- 특정 리소스를 배포할 때 배포할 Azure 지역을 선택해야 경우가 있다
(특정 VM 크기 또는 스토리지 형식을 포함한 일부 서비스 또는 기능은 특정 Azure 지역에서만 사용 가능하다)
- AD, Traffic Manager, DNS와 같이 지역을 선택할 필요 없는 글로벌 Azure 서비스도 있다
- 현재 Azure를 상업적으로 이용 할 수 있는 국가/지역은 140여개가 존재한다

<특수지역>

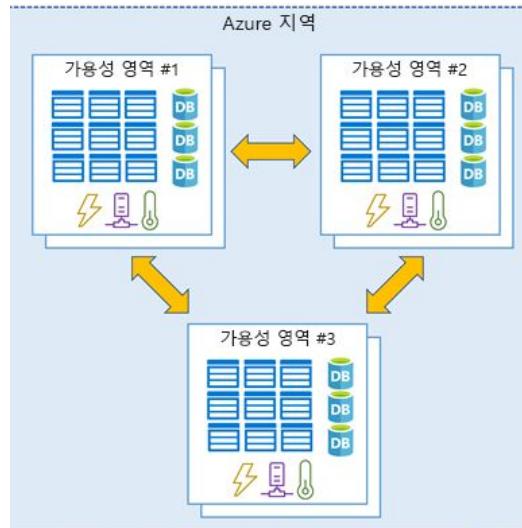
- US DoD 중부, US Gov 버지니아, US Gov 아이오와 등: 미국 정부 기관 및 파트너를 위한 물리적 및 논리적 네트워크로 격리된 Azure 인스턴스입니다. 이러한 데이터 센터는 선별된 미국인이 운영하며 추가 규정 준수 인증서를 포함하고 있습니다.
- 중국 동부, 중국 북부 등: 이러한 지역은 Microsoft 및 21Vianet 간의 고유한 파트너십을 통해 사용할 수 있으며, Microsoft에서 데이터 센터를 직접 관리하지 않습니다.

<Azure 지리적 위치>

- 데이터 상주성 및 규정 준수 경계를 유지하는 두 개 이상의 Azure 지역을 포함하고 있는 별도의 시장을 의미
- 아메리카, 유럽, 아시아 태평양, 중동 및 아프리카
- 각 Azure 지역은 한 지리적 위치에 속하며 특정 서비스 가능성, 규정 준수 및 데이터 상주/주권 규칙이 적용된다

Azure 가능성 영역(AZ)

- Azure 지역 내에서 물리적으로 분리된 데이터센터이다
- 각 가능성 영역은 독립된 전원, 냉각 및 네트워킹을 갖춘 하나 이상의 데이터 센터로 구성된다
- 가능성 영역은 격리 경계로 설정되며, 한 영역이 다운되어도 다른 영역은 작동하는 원리이다
- 고속 프라이빗 광 네트워크를 통해 각 가능성 영역은 연결된다
- 한 영역 내에 컴퓨팅, 스토리지, 네트워킹 및 데이터 리소스를 공동 배치하고 다른 영역에 복제하여 애플리케이션 아키텍처에 고가용성을 구현한다.(영역간의 데이터 전송에는 비용이 발생)
- 일부 지역은 가능성 영역이 지원되지 않는다
 - 영역 서비스 - 특정 영역에 리소스를 고정합니다(예: 가상 머신, 관리 디스크, IP 주소).
 - 영역 중복 서비스 - 플랫폼이 영역에서 자동으로 복제됩니다(예: 영역 중복 스토리지, SQL Database).



Azure 지역 쌍

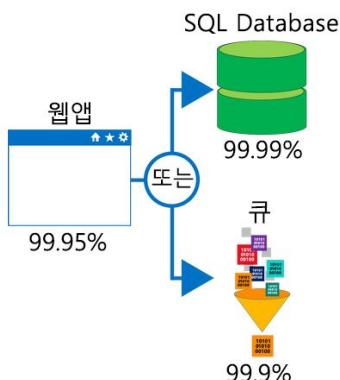
- 각 Azure 지역은 300마일 이상 떨어져 있는 동일한 지리적 위치 내의 다른 Azure 지역과 항상 쌍을 이룬다
- 이 방법으로 한 지리적 위치에서 가상 머신 스토리지 같은 리소스를 복제 할 수 있으며, 두 Azure 지역에 발생하는 자연재해 또는 물리적 중단 등의 이벤트 때문에 생기는 중단 가능성을 줄일 수 있다
- 지역 쌍은 직접 연결되고, 동시에 재해를 입는 피해를 피할 수 있도록 충분히 멀리 떨어져 있기 때문에 안정적인 서비스 및 데이터 중복성을 제공한다

SLA

- Premium에서는 99.9%의 가용성을 보장한다
- 무료 계층의 SLA는 제공하지 않는다
- SLA의 보장된 서비스 내용을 받지 못할 시에는 요금의 일부에 대한 크레딧을 자동으로 다음달 청구서에서 혜택을 받을 수 있다
- SLA에서 보장되는 것은 '가동시간','성능'이다
- 유료 Azure 서비스의 SLA 보장 가동 시간은 최소 99.9%이다
- 다중 AZ는 내결함성을 제공하고 다중지역은 재해복구를 제공하므로 리소스가 여러 지역에 걸쳐 있으면 SLA가 증가한다
- SLA는 구독이 아닌 서비스를 위한 것이다

복합 SLA

- SLA는 Azure 고객에게 특정 성능 표준을 제공하겠다는 MS 약정을 설명한다
- 개별 Azure 제품 및 서비스에 대한 SLA가 존재한다
- 개별 서비스의 SLA는 성능목표,작동시간 및 연결 보증, 서비스 크레딧 이라는 특징을 가지고 있다
- 여러 서비스 제품 간에 SLA를 결합 할 때 얻은 SLA를 복합 SLA라고 한다
- 복합 SLA는 결합 할 서비스간의 SLA의 곱이다
- 복합 SLA는 단일 SLA보다 실패할 확률이 커지는데, 이는 대체 경로를 만들어서 SLA를 높일 수 있다



구독(=user?)

- 구독은 사용자가 가입한 순간 자동으로 생성된다
- Azure에서 리소스를 프로비저닝하는데 사용되는 논리적 컨테이너이다
- VM, 데이터베이스 등 모든 리소스에 대한 세부 정보를 보관한다
- Azure 리소스를 만들 때 속한 구독을 식별한다
- 구독간의 리소스의 이전은 Azure portal을 이용하여 할 수 있다
- 여러 구독을 가질 수 있지만 제한이 존재하고, 하나의 관리자 계정으로 이루어진다
- Github와 같은 다른 계정들도 구독에 접근이 가능하다
- 리소스 또는 청구관리를 위해서 다음과 같은 추가 구독을 생성 할 수 있다
- Azure 및 해당 서비스를 사용할 수 있는 액세스 수준, 종량제 액세스의 경우 신용카드를 사용하여 Azure 구독을 설정한다

- 구독에는 여러 가지의 유형이 존재하고, 각 계정은 여러 구독을 사용할 수 있다

1. 환경

리소스를 관리할 때 개발 및 테스트, 보안을 위한 별도의 환경을 설정하거나 규정 준수 상의 이유로 데이터를 격리 할 수 있다. 리소스의 액세스 제한은 구독 수준으로 발생하기 때문에 유용하다

2. 조직구조

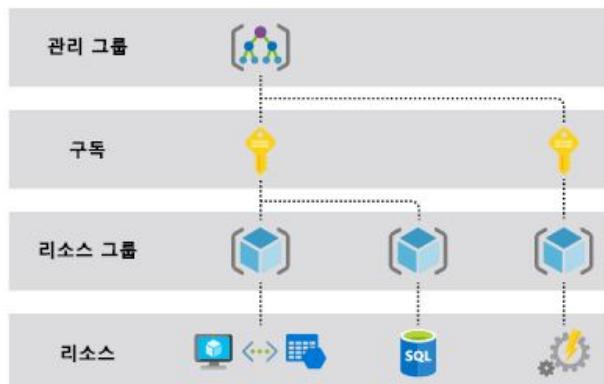
여러 조직 구조를 반영하는 구독을 만들 수 있다. 각 부서마다 리소스를 제한하거나, 권한을 허용하는 구독을 만들 수도 있다. 이와 같은 설계방식을 통해 사용자가 프로비저닝하는 리소스에 대한 액세스를 제어할 수 있다

3. 청구

비용은 구독 수준에서 먼저 집계되므로 사용자의 요구에 따라 비용을 관리하고 추적하는 구독을 만들어 청구의 역할만 위임할 수 있다

4. 구독제한

각 구독은 하드웨어에 바인딩 되기 때문에 10개의 제한이 있다. 이런 경우 Azure service에 새 지원 요청을 통해 구독의 수를 늘릴 수 있다



Azure 관리도구

- 다양한 도구 및 플랫폼을 사용하여 Azure를 구성하고 관리 할 수 있다
 - **Azure Portal** - GUI(그래픽 사용자 인터페이스)를 통해 Azure 조작
 - **Azure PowerShell 및 Azure CLI**(명령줄 인터페이스) - 명령줄 및 자동화 기반으로 Azure 조작
 - **Azure Cloud Shell** - 웹 기반 명령줄 인터페이스
 - **모바일 디바이스에서 리소스를 모니터링하고 관리하기 위한 Azure 모바일 앱**

1. Azure Portal

- 모든 웹 브라우저를 통해 액세스 할 수 있는 공용 웹 사이트이다
- Azure 계정으로 로그인만 하면 사용 가능한 모든 서비스를 생성, 관리 및 모니터링 할 수 있다
- Portal은 반복 작업을 자동화하는 방법을 제공하지 않는다
- 이 프로세스에는 복잡한 작업인 경우 포털 접근에 시간이 오래 걸리고 오류가 발생 할 수 있다



2. Azure Powershell

- 환경 내에서 Azure 구독에 연결하고 리소스를 관리 할 수 있다
- Windows, Linux 또는 macOS에서 실행되는 Powershell 또는 Powershell Core를 설치할 수 있는 모듈
- Powershell 또는 Powershell Core는 셸 창, 명령 구문 분석 등의 서비스를 제공한다
ex. 'Connect-AzAccount' 명령을 사용하여 Azure 계정에 로그인 한 다음, 'New-AzVM' 가상 머신을 만드는 명령을 제공한다
- 관리 스크립트 파일을 만들고 자동화 도구를 사용하는 반복작업을 자동화 할 수 있다

```

New-AzVM
  -ResourceGroupName "MyResourceGroup"
  -Name "TestVm"
  -Image "UbuntuLTS"
  ...
  
```

3. Azure CLI

- Azure에 연결하고 Azure 리소스에서 관리 명령을 실행하는 플랫폼 간 명령줄 프로그램
- Windows, Linux 또는 macOS에서 실행 할 수 있음
- Windows의 경우 cmd에서의 실행도 가능함
- 'az login' 명령을 사용하여 Azure에 로그인하고, 리소스 그룹을 만들고, 'az vm create' 명령어로 가상머신을 생성

```

az vm create \
--resource-group MyResourceGroup \
--name TestVm \
--image UbuntuLTS \
--generate-ssh-keys \
...

```



4. Azure Cloud shell

- Azure 리소스를 관리하기 위한 인증된 대화형 셸로, 브라우저에서 액세스 할 수 있음
- Bash나 Powershell 작업 방식에 가장 적합한 셸 환경을 유연하게 선택 할 수 있다
- 두 셸 간에 전환 할 수 있으며, Azure CLI와 Azure Powershell 모듈을 지원한다
- Bash는 기본적으로 Azure CLI로 설정되어 있지만 'pwsh' 명령어로 Linux용 Powershell Core로 전환 할 수 있다
- 이러한 관리 도구 외에도 다음과 같은 개발자 도구, 텍스트 편집기 및 기타 도구가 포함되어 있다

개발자 도구

- .NET Core
- Python
- Java
- Node.js
- 이동

편집기

- 코드(Cloud Shell 편집기)
- vim
- nano
- emacs

기타 도구

- git
- maven
- make
- npm
- 추가...

5. Azure 모바일 앱

- 해당 기능을 사용하면 IOS나 Android 휴대폰 또는 태블릿에서 모든 Azure 계정과 리소스를 액세스, 관리 및 모니터링 할 수 있다

Azure Marketplace

- 고객이 전 세계 우수 서비스 공급 기업에서 제공하는 Azure 인증 애플리케이션 및 서비스를 검색, 체험, 구매, 프로비저닝 하는 서비스
- 솔루션 카탈로그는 오픈 소스 컨테이너 플랫폼, 가상 머신 이미지, 데이터베이스, 애플리케이션 빌드 및 배포 소프트웨어, 개발자 도구, 위험 탐지, 블록 체인을 포함하여 다양한 산업 범주를 아우른다
- 해당 서비스를 사용하여 고객의 Azure 환경에 호스트되는 엔드투엔드 솔루션을 빠르고 안정적으로 프로비저닝 할 수 있다

Marketplace

The screenshot shows the Azure Marketplace interface. On the left, there's a sidebar with navigation links: '프라이빗 Marketplace(미리 보기)', '내 저장된 목록', '최근에 만들어짐', '서비스 공급자', '범주', '시작' (which is highlighted), and 'AI + 기계 학습'. The main area has a search bar at the top with placeholder text 'Marketplace 검색'. Below the search bar, there are three categories: 'Managed Services', 'Data#3', and 'Cloudetee Reliability'. Each category contains several service offerings with their names and brief descriptions.

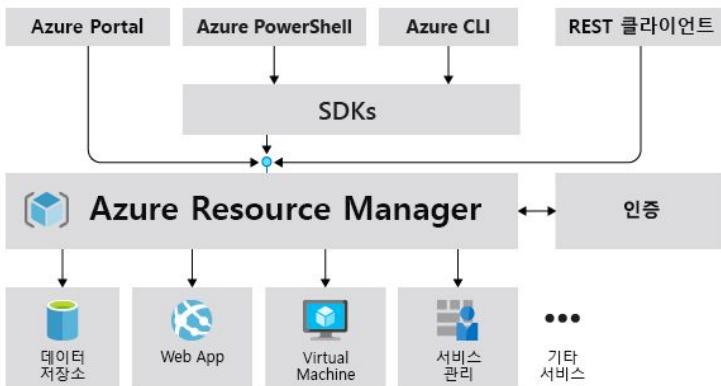
| Managed Services | Data#3 | Cloudetee Reliability |
|--|---|--|
| Aumatics Managed Services for your Azure Tenant | VIACode Managed Services for Azure VIACode Extend your IT team with VIACode Managed Services for Azure to improve your IT processes | Data#3 Azure Managed Services Data#3 Limited Data#3 Azure Managed Services |

Azure Resource Manager

- Azure 계정에서 리소스를 만들고 업데이트하고 삭제 할 수 있는 관리 계층을 제공
- 배포 이후 액세스 제어, 잠금 및 태그와 같은 관리 기능을 사용하여 리소스를 보호하고 구성한다
- 사용자가 Azure 도구(Azure portal, REST..) 및 API/SDK(Powershell,CLI)에서 요청을 받아 해당 요청을 작업을 수행하는 Azure 서비스에 인증하고 권한을 부여한다
- 모든 요청이 동일한 API(Resource Manager)를 통해 처리되므로 모든 여러 도구에서 일관적인 결과 및 기능을 볼 수 있다

리소스 관리자를 사용할 경우의 이점

- 스크립트가 아니라 선언적 템플릿을 통해 인프라를 관리합니다.
- 이 리소스를 개별적으로 처리하는 대신, 솔루션의 모든 리소스를 그룹으로 배포, 관리 및 모니터링합니다.
- 개발 수명 주기 전체에 걸쳐 솔루션을 다시 배포하고, 리소스가 일관된 상태로 배포된다고 확신할 수 있습니다.
- 리소스가 올바른 순서로 배포되도록 리소스 간의 종속성을 정의합니다.
- RBAC(역할 기반 액세스 제어)가 기본적으로 관리 플랫폼에 통합되어 있으므로 액세스 제어가 모든 서비스에 적용됩니다.
- 리소스에 태그를 적용하여 구독의 모든 리소스를 논리적으로 구성합니다.
- 동일한 태그를 공유하는 리소스 그룹에 대한 비용을 확인하여 조직의 청구를 명확히 합니다.



<리소스>

- 배포된 Azure 서비스를 사용자가 원하는 환경으로 실행 한 것을 리소스라고 하는 것 같음
- Azure를 통해 사용할 수 있는 관리 가능한 항목으로, 가상머신/스토리지 계정/웹앱/데이터베이스/가상 네트워크 등이 있다
- 리소스 그룹/구독/관리그룹/태그도 하나의 리소스에 포함된다

| □ 이름 ↑↓ | 형식 ↑↓ | 위치 ↑↓ |
|------------------------|----------------------|-------|
| □ cs110032000e2bb18f1 | 스토리지 계정 | 동남아시아 |
| □ dongbari | App Service | 동아시아 |
| □ dongbari | Application Insights | 동아시아 |
| □ test | App Service 계획 | 동아시아 |

<리소스 그룹>

- Azure 솔루션에 관련된 리소스를 보유하는 컨테이너이다
- 리소스 그룹은 조직에 가장 적합한 리소스를 그룹에 넣어 관리한다
- 리소스를 만들 때 리소스 그룹을 선택하여 사용자가 원하는 인프라를 구성한다
- 리소스 그룹의 모든 리소스는 동일한 수명 주기를 공유해야 한다
(다른 수명 주기를 가지고 있는 경우 다른 리소스 그룹에 배포해야함)
- 각 리소스는 하나의 리소스 그룹에만 포함되어야 한다
- 특정 리소스 그룹에서 다른 그룹에 리소스를 이동 시킬 수 있다
- 리소스 그룹의 리소스는 리소스 그룹과 다른 지역에 있을 수 있다(**위의 그림)
- 관리 작업에 대한 Access Control 범위를 지정하는 데 리소스 그룹을 사용 할 수 있다
(리소스 그룹을 관리하려면 Azure 정책, RBAC 역할, 리소스 잠금 할당 사용)
- 리소스 그룹에 대해 태그를 지정할 수 있다
(포함된 리소스에는 태그가 상속되지 않지만 권한은 상속이 된다)
- 리소스는 다른 리소스 그룹의 리소스에 연결 할 수 있다
- 각 리소스 그룹에는 최대 800개까지의 리소스를 배포 할 수 있다

- 특정 리소스는 리소스 그룹 외부(구독, 관리 그룹, 테넌트)에 배포 할 수 있다

<리소스 공급자>

- Azure 리소스를 제공하는 서비스이다
ex. Microsoft.Compute, Microsoft.Storage ...

<리소스 매니저 템플릿>

<https://docs.microsoft.com/ko-kr/azure/azure-resource-manager/templates/overview>

- 리소스 그룹, 관리 그룹 또는 테넌트에 포함 시킬 하나 이상의 리소스를 정의하는 JSON 파일이다
- 하나 이상의 리소스를 일관되고 반복적으로 배포하는 데 사용한다

<리소스 잡금>

- 모든 리소스에 적용하여 수정 또는 삭제를 막을 수 있는 설정이며, 삭제 또는 읽기전용으로 설정 할 수 있다
- 삭제는 리소스를 삭제하는 기능을 제외하고 리소스에 대한 모든 작업을 허용합니다
- 읽기전용은 리소스 읽기 작업만 허용하고 리소스의 삭제나 수정을 차단한다
- 리소스 잡금은 구독, 리소스 그룹 및 개별 리소스에 적용할 수 있으며 상위 수준에서 적용할 경우 상속된다

Azure Advisor

- Azure에 내장된 무료 서비스로, 고가용성/보안/성능/뛰어난 운영/비용에 대한 권장 사항을 제공한다
- 배포된 서비스를 분석하여 해당 영역에서 환경을 개선할 방법을 찾는다
- 포털에서 추천을 보거나 PDF 또는 CSV 형식으로 다운로드 할 수 있다
- 사전 대응이 가능하고, 실행 가능하고, 맞춤형 모범 사례 추천 가져오기
- 전체적인 Azure 비용을 줄일 수 있는 기회를 모색하면서 리소스의 성능, 보안 및 고가용성 개선
- 온라인으로 작업이 제안되는 추천 가져오기

퍼블릭 및 프라이빗 미리 보기 기능

- MS는 평가 목적으로 Azure 기능의 미리 보기 제공하여 사용자가 미리 베타 및 기타 시험판 기능, 제품, 서비스, 소프트웨어, Azure 지역을 테스트 할 수 있다

<퍼블릭 미리보기>

- 평가를 목적으로 모든 Azure 고객에게 제공하는 미리보기 기능

<프라이빗 미리보기>

- 평가를 목적으로 특정 Azure 고객에게만 제공하는 미리보기 기능

정적 웹앱 만들기(미리 보기)

The screenshot shows the 'Basic' tab of the 'Create a static web app' wizard. It includes fields for 'Subscription' (selected), 'Resource group' (selected), 'Name' (e.g., 'myapp'), 'Region' (selected), 'SKU' (selected), and 'Create'. Below this, there's a 'Static app settings' section with 'Name' and 'Region' fields, and a 'GitHub' button.

| 기본 | 태그 | 검토 + 만들기 |
|-------------|--------------|-------------|
| 구독 * | 무료 체험 | |
| 리소스 그룹 * | 새로 만들기 | |
| 정적 웹앱 세부 정보 | | |
| 이름 * | 정적 웹앱의 이름 입력 | |
| 지역 * | | |
| SKU | 무료 | |
| 소스 제어 세부 정보 | | |
| GitHub 계정 | | GitHub로 로그인 |

Azure 서비스

<https://azure.microsoft.com/ko-kr/services/>

컴퓨팅

- 애플리케이션 및 서비스를 호스팅 하는 주문형 컴퓨팅 서비스
- 가상 머신 및 컨테이너를 통해 멀티 코어 프로세서, 슈퍼 컴퓨터 등의 리소스를 제공한다
- 인프라(서버) 설정 또는 구성이 필요하지 않고 앱을 실행하는 서비스 컴퓨팅도 제공한다
- 리소스는 요청 시 제공되며, 수분 수초 이내에 만들 수 있다
- 사용자는 사용한 리소스에 대해 사용시간만큼만 요금을 지불하면 된다
- 컴퓨팅을 실현하는 기술에는 가상머신(VM), 컨테이너, App Service, 서비스 컴퓨팅이 있다

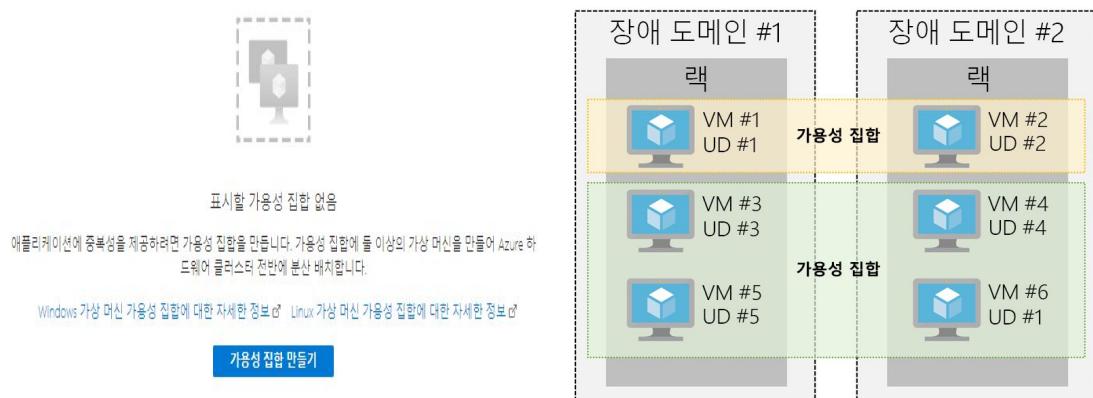
| 서비스 이름 | 서비스 기능 |
|----------------------------------|--|
| Azure Virtual Machines | Azure에서 호스팅되는 Windows 또는 Linux VM(가상 머신) |
| Azure Virtual Machine Scale Sets | Azure에서 호스팅되는 Windows 또는 Linux VM의 크기 조정 |
| Azure Kubernetes Service | 컨테이너화된 서비스를 실행하는 VM 클러스터 관리를 사용하도록 설정 |
| Azure Service Fabric | 분산형 시스템 플랫폼. Azure 또는 온-프레미스에서 실행 |
| Azure Batch | 병렬 및 고성능 컴퓨팅 애플리케이션을 위한 관리 서비스 |
| Azure Container Instances | 서버 또는 VM을 프로비저닝하지 않고 Azure에서 컨테이너화된 앱 실행 |
| Azure Functions | 이벤트 기반의 서비스 컴퓨팅 서비스 |

<가상머신(Virtual Machine, VM)> IaaS

- 물리적 컴퓨터의 소프트웨어 에뮬레이션(복제), 가상 프로세서/메모리/스토리지/네트워킹 리소스가 포함된다.
- OS를 호스트하며, 물리적 컴퓨터처럼 소프트웨어를 설치하고 실행 할 수 있다. 원격 데스크톱 클라이언트를 사용하여, 실제처럼 가상 머신을 사용하고 제어할 수 있다
- 미리 구성된 가상머신 이미지를 사용하면 짧은 시간 안에 프로비저닝이 가능하다
- 가상 머신을 그룹화하여 고가용성, 확장성 및 중복성을 제공하는 기능을 갖고있다
(가용성 집합, Virtual Machine Scale Sets, Azure Batch)

1. 가용성 집합

- 그룹화 된 가상머신의 서비스 가용성을 보장하기 위해서 장애도메인과 업데이트 도메인으로 가상 머신을 구성하는 집합
- 가용성 집합을 사용하면 전원 및 네트워크 리소스가 있는 서버 랙을 포함하는 최대 3개의 장애도메인, 5개의 업데이트 도메인이(최대 20개) 제공된다
- 가용성 집합에 대한 비용은 따로 없고, 가용성 집합 내의 가상 머신에 대해서만 요금이 부과된다
- 장애도메인과, 업데이트 도메인에는 순차적으로 자동 배치된다
- 장애도메인(Fault Domain)
 - : 동일한 전원과 네트워크 스위치를 사용하는 가상머신의 집합, 하나의 물리적인 랙(Rack)
 - : 업데이트 도메인(Update Domain)
 - : Azure의 계획된 유지 관리로 인해서 운영 중인 호스트 업데이트를 진행할 때, 동시에 진행되는 하나의 호스트 그룹, 동시에 2개 이상의 업데이트 도메인에서 업데이트 하지 않기 때문에 유지 보수로 인한 호스트 재기동과 같은 상황에서 서비스를 유지 할 수 있다



2. Virtual Machine Scale Sets

- 부하 분산된 동일한 가상 머신 그룹을 만들고 관리 할 수 있다
- 여러 가상 머신을 복제한 경우 웹사이트에서 가상 머신의 여러 인스턴스 간에 요청을 라우팅 하는 작업을 자동으로 수행한다
- 많은 수의 가상머신을 중앙에서 관리, 구성 및 업데이트 하므로 고가용성 애플리케이션을 제공 할 수 있다
- 가상머신 인스턴스의 수는 요구 또는 정의된 일정에 따라 자동으로 확장/축소 할 수 있다
- 컴퓨팅, 빅 데이터 및 컨테이너 작업과 같은 영역에 대한 대규모 서비스를 구축 할 수 있다

3. Azure Batch

- 수십, 수백, 수천 개의 가상 머신으로 확장하고, 대규모 작업을 예약하고 컴퓨팅을 관리 할 수 있다

작업을 실행할 준비가 된 경우, Batch에서 다음 작업을 수행합니다.

- 컴퓨팅 가상 머신 풀을 시작합니다.
- 애플리케이션 설치 및 준비 데이터를 설치합니다.
- 사용자의 여러 태스크를 포함하는 작업을 실행합니다.
- 오류를 식별합니다.
- 작업을 큐에 다시 대기합니다.
- 작업이 완료되면 풀을 축소합니다.

<컨테이너>

- 애플리케이션을 실행하기 위한 가상화 환경. 가상머신과 마찬가지로 호스트 운영체제에서 실행된다.
- 단일 호스트 머신에서 여러 애플리케이션을 실행하려는 경우에 사용한다
- 컨테이너는 보안이 설정되고 격리되므로 각 앱의 별도의 서버가 필요하지 않는다
- VM과의 큰 차이점은 컨테이너 내부에서 실행되는 앱의 운영체제를 포함하지 않는다. 대신, 애플리케이션을 실행하고 컨테이너를 실행하는 기존 호스트 OS를 사용하는 데 필요한 라이브러리와 구성요소를 포함한다
ex) 리눅스 커널이 있는 서버에서 컨테이너 5개를 실행하는 경우 컨테이너 5개와 그 안에 있는 앱 모두 동일한 리눅스 커널을 공유한다
- Docker 컨테이너(표준화된 컨테이너 모델)를 지원하고 Azure에서 컨테이너를 관리하는 다양한 서비스를 제공한다
- 컨테이너는 마이크로 서비스 아키텍처를 사용하여 솔루션을 만드는 데 사용되는데, 이 아키텍처에서는 솔루션을 더 작고 독립적인 조각으로 분할 할 수 있다
ex. 웹 사이트를 프런트 엔드로 호스팅하는 컨테이너, 백엔드를 호스팅하는 컨테이너 및 스토리지용 컨테이너로 분할 할 수 있다

1. ACI(Azure Container Instances)

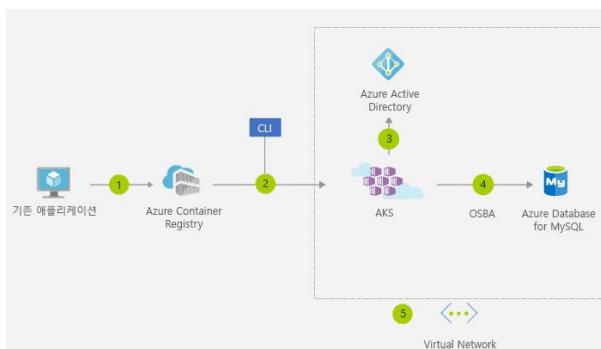
- Azure에서 컨테이너를 실행하는 가장 빠르고 쉬운 방법, 가상 머신을 관리하거나 추가 서비스를 구성할 필요가 없다
- 컨테이너를 업로드하고 자동 탄력적 확장을 통해 직접 실행할 수 있는 PaaS 제품

2. AKS(Azure Kubernetes Service)

- AKS는 여러 컨테이너가 있는 분산 아키텍처를 사용하는 완벽한 컨테이너용 오픈스토레이션 서비스이다
- 많은 컨테이너를 자동화, 관리 및 상호작용하는 작업을 '오픈스토레이션'이라고 한다



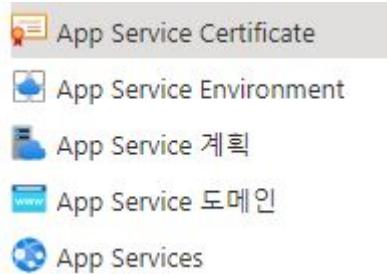
컨테이너로 앱 마이그레이션



- 기존 애플리케이션을 컨테이너로 이동하고 AKS 내에서 이를 실행할 수 있다
- Azure AD, 액세스 SLA 지원 Azure 서비스와의 통합을 통해, OSBA(Open Service Broker for Azure)를 통해 액세스를 제어할 수 있다

<Azure App Service>

- 웹 기반 애플리케이션을 호스트하도록 설계된 Azure의 PaaS 제품이다.
- 인프라를 관리할 필요 없이 원하는 프로그래밍 언어로 웹앱, 백그라운드 작업, 모바일 백엔드 및 RESTful API를 빌드하고 호스트 할 수 있다
- 자동 확장 기능과 고가용성을 제공한다
- Windows 및 Linux 환경을 모두 지원하며, Azure DevOps/Git 리포지토리, GitHub에서 자동화된 배포를 사용하여 지속적인 배포 모델을 지원한다



<서비스 컴퓨팅>

- 코드를 실행하는, 클라우드에 호스트된 실행환경이지만 기본 호스팅 환경을 완전히 추상화한다
- 서비스 인스턴스를 만들고 코드를 추가하기만 하면 된다
- 인프라는 사용자의 책임이 아니고, 크기 조정 및 성능이 자동으로 처리되며, 사용하는 리소스에 대해서만 요금이 청구된다
- 서비스 컴퓨팅 다음의 두 가지 컴퓨팅 구현을 제시한다

1. Azure Functions

- 기본 플랫폼이나 인프라가 아닌, 서비스를 실행하는 코드에 관해서만 관심이 있는 경우 사용하는 것이 이상적이다
- REST 요청, 타이머 또는 다른 Azure 서비스로부터 받은 메세지를 통해 이벤트에 대한 응답으로 작업을 수행해야 하는 경우, 해당 작업을 수초 이내에 빠르게 완료 할 수 있는 경우에 사용된다
- 수요에 따라 자동으로 크기가 조정되므로 수요가 가변적일 때 사용하는 것이 좋다
- 함수는 트리거 때 코드를 실행하고, 함수가 완료되면 리소스를 할당 해체하기 때문에 함수가 실행되는 CPU 시간에 대한 요금만 발생한다

2. Azure Logic Apps

- 특정 이벤트가 발생하거나 사용 가능한 새 데이터가 특정 기준을 충족할 때 실행되는 트리거를 통해 시작된다
- 워크로드가 주기적으로 실행되는 빈도를 개발자가 지정할 수 있도록 많은 트리거가 기본적인 일정 예약 기능을 제공한다
- 트리거가 실행될 때마다 Logic Apps 엔진은 워크플로의 작업을 실행하는 논리 앱 인스턴스를 만든다
- 워크플로는 알려진 워크플로 스키마를 사용하여 JSON 파일로 지속된다

| | Functions | Logic Apps |
|----------|---|--|
| 시스템 상태 | 일반적으로 상태 비저장이지만 Durable Functions가 상태를 제공함 | 상태 저장 |
| 개발 | 코드 중심(병렬적) | 디자이너 중심(선언적) |
| 연결 | 약 12가지의 기본 제공 바인딩 형식 정보, 사용자 지정 바인딩에 대한 코드 작성 | 대규모의 커넥터 컬렉션, B2B 시나리오용 엔터프라이즈 통합 팩, 사용자 지정 커넥터 빌드 |
| 작업 | 각 작업은 Azure 함수입니다. 작업 함수에 대한 코드 작성 | 즉시 사용 가능한 작업의 대규모 컬렉션 |
| 모니터링 | Azure Application Insights | Azure Portal, Log Analytics |
| 관리 | REST API, Visual Studio | Azure Portal, REST API, PowerShell, Visual Studio |
| 실행 컨 텍스트 | 로컬로 또는 클라우드에서 실행 가능 | 클라우드에서만 실행합니다. |

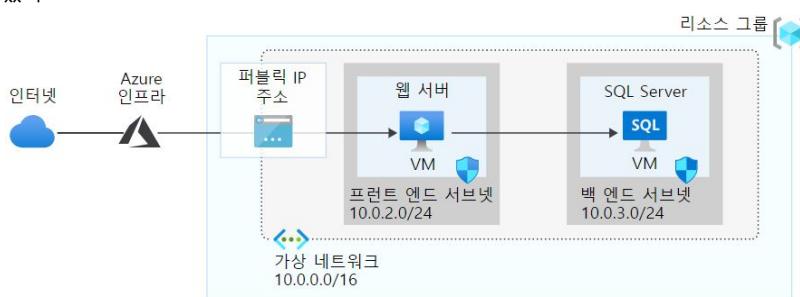
네트워킹

- 컴퓨팅 리소스를 연결하고 애플리케이션에 대한 액세스를 제공
- 온-프레미스 네트워크와 Azure Virtual Network 인스턴스 간에 대기 시간이 짧고 고대역폭 연결이 필요로 하다면, Azure 게이트웨이를 통해 VPN 연결을 사용하거나 Azure ExpressRoute를 통한 전용 연결을 사용할 수 있다.

| 서비스 이름 | 서비스 기능 |
|--------------------------------|--|
| Azure Virtual Network | 수신 VPN(가상 사설망) 연결에 VM을 연결합니다. |
| Azure Load Balancer | 애플리케이션 또는 서비스 엔드포인트에 대한 인바운드 및 아웃바운드 연결의 균형을 맞춥니다. |
| Azure Application Gateway | 애플리케이션 보안을 강화하는 동시에 앱 서버 팜 제공을 최적화합니다. |
| Azure VPN Gateway | 고성능 VPN 게이트웨이를 통한 Azure 가상 네트워크에 액세스합니다. |
| Azure DNS | 매우 빠른 DNS 응답과 매우 높은 도메인 가용성을 제공합니다. |
| Azure Content Delivery Network | 전 세계 고객에게 고대역폭 콘텐츠를 제공합니다. |
| Azure DDoS Protection | Azure에서 호스트되는 애플리케이션을 DDoS(배포된 서비스 거부) 공격으로부터 보호합니다. |
| Azure Traffic Manager | 전 세계 Azure 지역에 네트워크 트래픽을 분산합니다. |
| Azure ExpressRoute | 고대역폭 전용 보안 연결을 통해 Azure에 연결합니다. |
| Azure Network Watcher | 시나리오 기반 분석을 사용하여 네트워크 문제를 모니터링하고 진단합니다. |
| Azure Firewall | 확장성에 제한이 없고 보안 수준이 높은 고가용성 방화벽을 구현합니다. |
| Azure 가상 WAN | 로컬 사이트와 원격 사이트를 연결하는 통합 WAN(광역 네트워크)을 구축합니다. |

1. Azure Virtual Network

- 실제 온-프레미스 네트워크의 구조를 에뮬레이터 하는 복잡한 가상 네트워크를 구축 할 수 있다
- 클라우드 기반 가상 네트워크를 프로비저닝 할 수 있다
- 대부분의 가상 네트워크는 프라이빗 네트워크로 간주된다
- 온-프레미스 네트워크와 통합되는 하이브리드 가상 네트워크를 만들 수 있다
- 다른 가상 네트워크 및 온-프레미스 네트워크와 통신 할 수 있는 프라이빗 네트워크를 구축 할 수 있다
- 일반 네트워크를 이용할때처럼 서브넷 지정을 사용하여 IP 주소 범위를 세그먼트화하고 해당 서브넷에 제공하는 주소 지정 방법을 제어 할 수 있다
- 가상 네트워크는 단일 지역으로 범위가 제한되지만 피어링을 통해 여러 지역의 가상 네트워크를 연결 할 수 있다
- 가상 네트워크는 하나 이상의 서브넷으로 분할 될 수 있고, 서브넷을 통해 개별 세션의 리소스를 구성하고 보호 할 수 있다

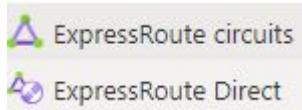


2. NSG(Network Security Group)

- 포함된 Azure 리소스에 대한 인바운드 네트워크 트래픽을 허용/차단하는 네트워크 보안 그룹
- 클라우드 수준의 방화벽이라고 생각하면 된다
- 특정 port, 서비스로부터 들어오는 트래픽을 허용/차단 설정을 할 수 있다

3. Azure ExpressRoute

- 일반적인 VPN Gateway 연결보다 훨씬 더 높은 대역폭을 사용하는, 온-프레미스 네트워크와 클라우드 간의 전용 회로이다.
- ExpressRoute는 안전한 지점간의 서비스이다
- 전용 회로는 연결 파트너가 호스팅하며, 복원력이 뛰어난 연결을 제공한



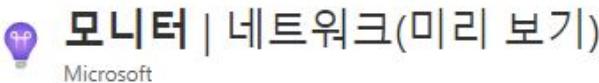
4. Azure Network Watcher(모니터링)

- 이용 중인 Azure 서비스에서 패킷 데이터를 캡처하거나 네트워크 트래픽 패턴의 데이터 흐름을 이해하고 사용 중인 네트워크의 네트워크 관련 문제를 해결하는 네트워크 모니터링 서비스



5. NPM(네트워크 성능 모니터)

- 네트워크 상태를 모니터링 및 보고하고, 네트워크 성능에 대한 유익한 정보를 제공하며, 애플리케이션 간의 연결 상태를 보고하는 기능이다
- 해당 기능은 클라우드 기반이지만 온-프레미스 네트워크 포함 모두 모니터링하는 하이브리드 서비스이다

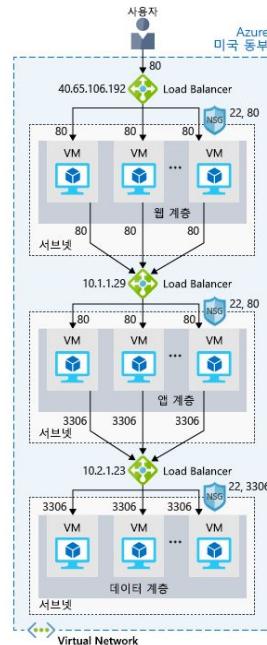


6. Azure DNS

- 등록된 도메인 이름을 Azure 인프라를 사용하여 호스트하는 서비스
- 일반 Azure 로그인 자격 증명을 사용하여 A, AAAA, CNAME, SOA, NS, MX 같은 DNS 레코드를 관리할 수 있다
- Azure DNS에서 제공하는 주요 이점 중 하나는 A, AAAA, CNAME 레코드를 사용 할 수 있는 별칭 레코드를 사용한다는 것이다. 별칭을 사용하면 Azure 리소스에 트래픽을 라우팅 할 수 있다

7. Azure Load Balancer

- 사용자를 위한 유지 관리를 담당하기 위해 MS에서 제공하는 부하 분산 장치 서비스
- 인바운드 및 아웃바운드 시나리오를 지원하고, 짧은 대기 시간과 높은 처리량을 제공하고, 모든 TCP/UDP 애플리케이션에 대해 수백만 개의 흐름을 확장한다
- 들어오는 인터넷 트래픽, Azure 서비스 간 내부 트래픽, 특정 트래픽을 포트에 전달 또는 가상 네트워크 내 VM의 아웃바운드 연결에 부하 분산 장치를 사용 할 수 있다



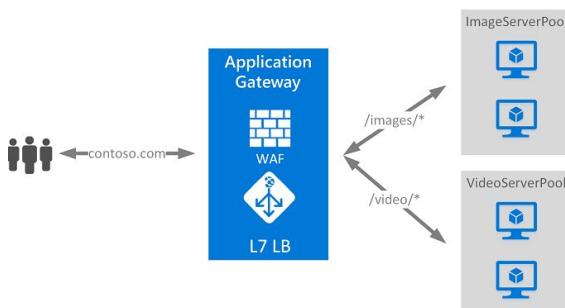
8. Azure Application Gateway

- 웹 애플리케이션 용으로 설계된 부하 분산 장치이다
- 전송 수준(TCP)에서 Azure Load Balancer를 사용하고, 정교한 URL 기반 라우팅 규칙을 적용하여 여러 고급 시나리오를 지원한다
- 이러한 유형의 라우팅은 HTTP 메세지의 구조를 이해한다고 해서 애플리케이션 레이어(L7) 부하 분산이라고 한다

- 모든 트래픽이 HTTP인 경우 해당 서비스를 사용하는 것이 잠재적으로 더 나은 옵션이다

간단한 부하 분산 장치를 통해 Azure Application Gateway를 사용할 경우의 장점은 다음과 같습니다.

- 쿠키 선호도. 동일한 백 엔드 서버에서 사용자 세션을 유지하려는 경우에 유용합니다.
- SSL 종료. Application Gateway는 사용자의 SSL 인증서를 관리하고 암호화되지 않은 트래픽을 백 엔드 서버로 전달하여 암호화/암호 해독 오버헤드를 방지할 수 있습니다. 또한 필요한 애플리케이션에 완벽한 엔드투엔드 암호화를 지원합니다.
- 웹 애플리케이션 방화벽. 애플리케이션 게이트웨이는 네트워크 인프라에 대한 악의적인 공격을 검색하는 세부적인 모니터링 및 로깅을 제공하는 정교한 방화벽(WAF)을 지원합니다.
- URL 규칙 기반 경로. Application Gateway를 사용하면 URL 패턴, 대상 IP 주소 및 포트에 해당하는 원본 IP 주소 및 포트에 따라 트래픽을 라우팅할 수 있습니다. 이는 _콘텐츠 전송 네트워크_를 설정하는 경우에 유용합니다.
- HTTP 헤더 다시 쓰기. 각 요청의 인바운드 및 아웃바운드 HTTP 헤더에서 정보를 추가하거나 제거하여 중요한 보안 시나리오를 구현하거나 서버 이름과 같은 민감한 정보를 스크립팅할 수 있습니다.



9. CDN (콘텐츠 전송 네트워크)

- 사용자에게 웹 콘텐츠를 효율적으로 제공할 수 있는 서버의 분산 네트워크이다
- 대기시간을 최소화하기 위해 로컬 지역의 사용자에게 콘텐츠를 배달하는 방식이다
- Azure 또는 다른 위치에서 호스팅 할 수 있다
- 전 세계에 전략적으로 배치된 물리적 노드에 콘텐츠를 캐시하고 최종 사용자에게 더 나은 성능을 제공할 수 있다
- 일반적인 사용 시나리오는 멀티미디어 콘텐츠가 포함된 웹 애플리케이션, 특정 지역의 제품 런칭 이벤트 또는 특정 지역에 높은 대역폭 요구 사항이 예상되는 모든 이벤트가 포함된다

10. Azure Traffic Manager

- 사용자에게 가장 가까운 DNS 서버를 사용하여 사용자 트래픽을 전역적으로 분산된 엔드포인트로 보낸다
- 클라이언트와 서버 간에 전달되는 트래픽을 확인하지 않는 대신 클라이언트 웹 브라우저를 기본 설정 엔드포인트로 보낸다
- ex. 대기시간이 짧은 엔드포인트로 라우팅 하는 경우

*** Load Balancer vs Traffic Manager

> Load Balancer는 동일한 지역 내의 트래픽을 분산시켜 서비스의 가용성과 복원력을 향상한

> Traffic Manager는 DNS 수준에서 작동하며 클라이언트를 기본 설정 엔드포인트로 보낸다

(이 엔드포인트는 사용자에게 가장 가까운 지역일 수 있다)

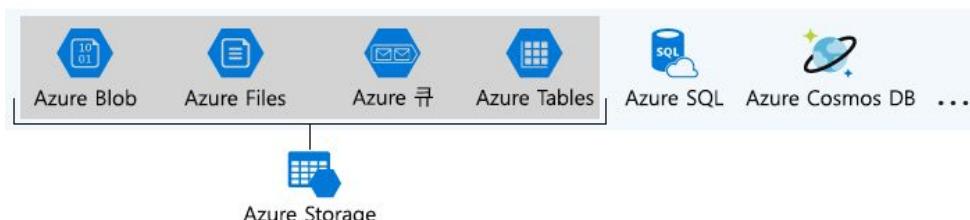
> Load Balancer는 응답하지 않는 VM을 감지하면 트래픽을 풀의 다른 VM으로 보내고, Traffic

Manager는 응답하지 않는 엔드포인트를 감지하면 트래픽을 응답하는 가장 가까운 다음

엔드포인트로 보낸다

스토리지

- 중복 및 복제 기능을 갖추고 있어 내구성과 가용성이 뛰어나다
- 자동 암호화와 역할 기반 액세스 제어를 통해 보안을 유지한다
- 스토리지에 제한이 없어 확장성이 뛰어나다
- 유지 관리 및 사용자에 대한 중요한 문제를 관리하고 처리한다
- HTTP/HTTPS를 통해 전 세계 어디서든 액세스 할 수 있다
- Azure SQL Database, Azure Cosmos DB, Azure Table Storage 등 여러 데이터베이스 옵션과 Azure Queue, Event Tables 등 메시지를 저장하고 보내는 방법, Azure Files 및 Azure Blob 같은 서비스를 사용하여 느슨한 파일도 저장한다



<데이터를 저장하는 데 Azure를 사용하는 이점>

- 예상치 못한 오류 또는 중단이 발생하는 경우 데이터 손실의 위험을 완화한다(자동화된 백업 및 복구)

- 데이터를 전 세계에 복제하여 예약된 유지 관리 또는 하드웨어 오류와 같은 계획되지 않은 이벤트에 대비해 데이터를 보호한다
- 데이터 이용에 대한 분석을 수행하는 기능을 지원한다
- 데이터를 암호화하여 높은 안정성을 보장하고, 데이터 액세스 할 수 있는 사용자에 대한 긴밀한 제어도 가능하다
- 필요한 거의 모든 데이터 형식(비디오 파일, 텍스트 파일, 가상 하드디스크 같은 이진 파일)을 저장 할 수 있고 관계형 DB나 NoSQL 같은 데이터에 대한 옵션도 다양하다
- 최대 32TB의 데이터를 해당 가상 디스크에 저장 할 수 있다. 이 기능은 동영상 및 시뮬레이션과 같은 대용량 데이터를 저장하는 경우 중요한 기능이다
- 데이터 사용 빈도에 따라 우선순위를 지정하는 스토리지 계층이다

<스토리지 계층>

1. 핫 스토리지 계층
자주 액세스하는 데이터를 저장하는 데 최적화되어 있는 계층
2. 쿨 스토리지 계층
드물게 액세스되고 최소 30일 동안 저장되는 데이터에 최적화되어 있는 계층
3. 보관 스토리지 계층
유연한 대기시간을 요구사항으로 최소 180일 동안 거의 액세스 및 저장되지 않은 데이터에 최적화되어 있는 계층

<데이터 형식>

1. 정형 데이터
스키마를 준수하는 데이터로, 모든 데이터에 동일한 필드 또는 속성이 존재한다(관계형데이터)
2. 반정형 데이터
테이블 행, 열에 고정되지 않고 데이터 계층 구조를 구성하고 제공하는 태그/키를 사용한다(NoSQL)
3. 비정형 데이터
포함될 수 있는 데이터 종류에 대한 제한이 없는 지정된 구조가 없는 데이터를 의미한다
ex. Blob 스토리지에 PDF, JPG, JSON, 동영상 등의 여러 파일이 포함될 수 있다

<암호화 및 복제>

- Azure는 암호화 및 복제 기능을 통해 보안 및 고가용성을 데이터에 제공한다
- 복제의 유형은 스토리지 계정을 만들 때 설정된다. 복제 기능은 데이터가 내구성이 있으며 항상 사용할 수 있는지 확인한다. Azure는 화재나 총수 같은 자연재해 및 기타지역 재해로부터 데이터를 보호하기 위한 지역 및 지리적 복제를 제공한다
- 암호화 유형
 1. 미사용 데이터에 대한 Azure SSE(Storage Service Encryption)를 사용하면 조직의 보안 및 규정 준수를 충족하도록 데이터를 보호화 할 수 있다 데이터를 저장하기 전에 암호화하고 데이터를 반환하기 전에 암호를 해독한다
 2. 클라이언트 쪽 암호화에서는 클라이언트 라이브러리에 의해 데이터가 이미 암호화되어 있다. Azure는 암호화된 상태로 미사용 데이터를 저장한 다음, 검색 중에 암호를 해독한다

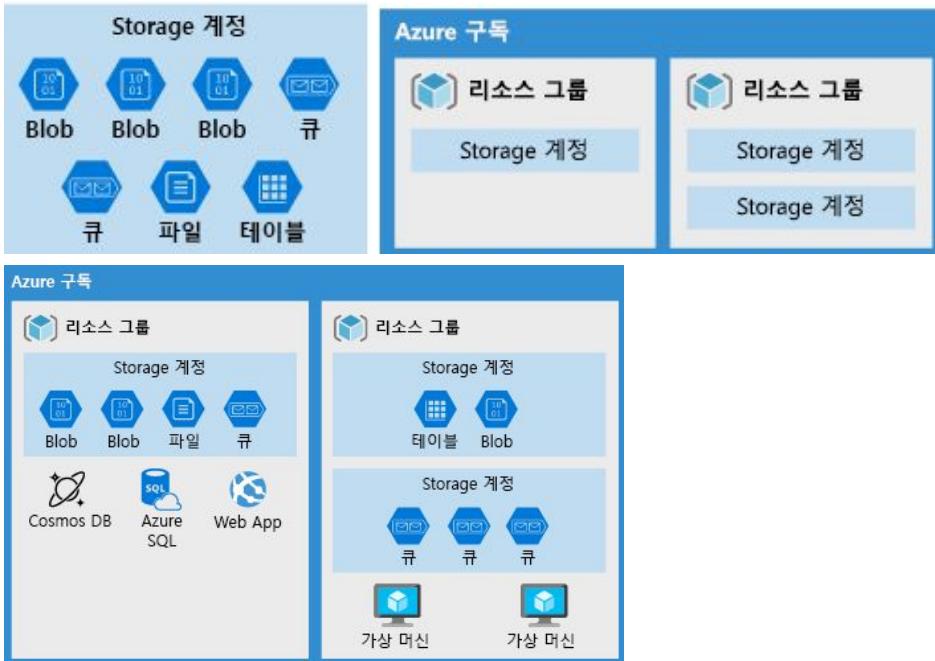
<온-프레미스와 Azure 데이터의 스토리지 비교>

| 필요 | 온-프레미스 | Azure 데이터 스토리지 |
|---------------------------|-------------------------------------|---|
| 규정 준수 및 보안 | 개인 정보 보호 및 보안에 필요한 전용 서버 | 클라이언트 쪽 암호화 및 미사용 암호화 |
| 정형 및 비정형 데이터 저장 | 전용 서버를 사용하는 추가 IT 리소스 필요 | Azure Data Lake 및 포털은 모든 형식의 데이터를 분석하고 관리합니다. |
| 복제 및 고가용성 | 추가 리소스, 라이선싱 및 서버 필요 | 사용 가능한 기본 제공 복제 및 중복 기능 |
| 애플리케이션 공유와 공유 리소스에 대한 액세스 | 파일 공유에는 추가 관리 리소스가 필요합니다. | 추가 라이선스 없이 사용 가능한 파일 공유 옵션 |
| 관계형 데이터 스토리지 | 데이터베이스 관리자 역할이 있는 데이터베이스 서버가 필요 | Database-as-a-Service 옵션 제공 |
| 분산 스토리지 및 데이터 액세스 | 비용이 많이 드는 스토리지, 네트워킹, 컴퓨팅 리소스 필요 | Azure Cosmos DB는 분산 액세스를 제공합니다. |
| 메시지 및 부하 분산 | 하드웨어 증복은 예산 및 리소스에 영향을 줍니다. | Azure Queue는 효과적인 부하 분산을 제공합니다. |
| 계층화된 스토리지 | 계층화된 스토리지를 관리하려면 기술 및 노동 기능이 필요합니다. | Azure는 계층화된 자동 데이터 스토리지를 제공합니다. |

<스토리지 계정>

- Azure Storage 서비스의 집합을 함께 그룹화하는 컨테이너
- 스토리지 계정에 데이터 서비스를 결합하면 해당 항목을 그룹으로 관리 할 수 있다
- 계정을 만들 때 지정한 설정 또는 생성 후에 변경한 설정은 계정의 모든 항목에 적용된다
- 스토리지 계정이 삭제되면 그 안에 모든 저장된 데이터를 삭제한다

- 스토리지 계정은 리소스이며 리소스 그룹에 포함된다
- Azure SQL 및 Azure Cosmos DB와 같은 다른 Azure 데이터 서비스는 독립적인 Azure 리소스로 관리되고 스토리지 계정에 포함될 수 없다



- 스토리지 계정 시 모든 스토리지 서비스에 적용되는 정책을 정의해야한다
(구독, 위치, 성능, 복제, 액세스 계층, 보안 전송 필요, 가상 네트워크)
- 정책 그룹 하나 당 하나의 스토리지 계정이 필요로하다(설정값이 하나만 달라도 또다른 계정이 필요하다)
- 각 정의한 설정값에 따라 다른 요금이 발생한다
- 스토리지 계정은 Azure Portal, Azure CLI, Azure Powershell, 관리 클라이언트 라이브러리 등의 관리도구로 생성이 가능하다

Storage 계정

Storage 계정

구독: 프로덕션
위치: 미국 서부
성능: 표준
복제: GRS
액세스 계층: 핫
보안 전송: 사용
가상 네트워크: 사용 안 함

구독: 프로덕션
위치: 북유럽
성능: 표준
복제: GRS
액세스 계층: 핫
보안 전송: 사용
가상 네트워크: 사용 안 함

기본 사항 네트워킹 데이터 보호 고급 태그 검토 + 만들기

Azure Storage는 기용성, 보안, 내구성, 확장성 및 중복성이 뛰어난 클라우드 스토리지를 제공하는 Microsoft 관리 서비스입니다. Azure Storage는 Azure Blob(객체), 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 참조

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

구독 * 무료 체험
리소스 그룹 * 새로 만들기

인스턴스 정보
기본 베패 모델은 최신 Azure 기능을 지원하는 Resource Manager입니다. 대신 클래식 배포 모델을 사용하여 배포하도록 선택할 수 있습니다. 클래식 배포 모델 선택

스토리지 계정 이름 * ○
위치 * (US) 미국 동부 ○ 표준 ○ 프리미엄
성능 ○ 계정 종류 ○ StorageV2(블록 v2)
복제 ○ RA-GRS(읽기 액세스 지역 중복 스토리지) ○ 끝 ○ 핫
Blob 액세스 계층(기본값) ○

서비스 이름

Azure Blob Storage

비디오 파일이나 비트맵 같은 대규모 개체를 위한 스토리지 서비스

Azure File 스토리지

파일 서버처럼 액세스하고 관리할 수 있는 파일 공유

Azure Queue 스토리지

애플리케이션 간 메시지를 큐에 넣고 안정적으로 전달하기 위한 데이터 저장소

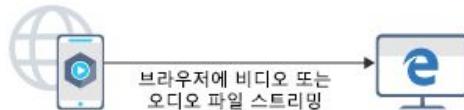
Azure Table 스토리지

スキ마와 관계없이 비정형 데이터를 호스팅하는 NoSQL 스토리지

1. Azure Blob Storage

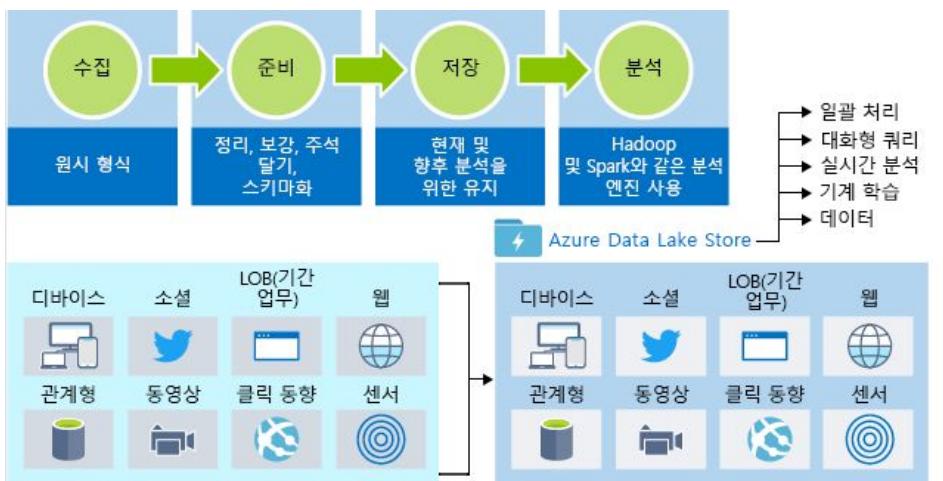
- 비정형 스토리지로, 포함 될 수 있는 데이터 종류에 대한 제한이 없다
- 확장성이 뛰어나며, 앱은 디스크의 파일을 사용(예:데이터 읽기 및 쓰기)하는 것과 동일한 방식으로 Blob을 사용한다
- 수천개의 동시 업로드, 대용량 비디오 데이터, 끊임없이 증가하는 로그 파일을 관리 할 수 있으며, 인터넷만 있다면 언제 어디서나 접속이 가능하다

- 하나의 Blob에 과학 기기에서 스트리밍 된 기가바이트의 이진데이터, 다른 애플리케이션용 암호화된 메시지 또는 개발 중인 앱에 대한 사용자가 지정한 형식의 데이터가 포함 될 수 있다
- 백업,재해 복구 및 보관용 데이터를 저장하기도 한다
- 최대 8TB의 가상 머신용 데이터를 저장 할 수 있다



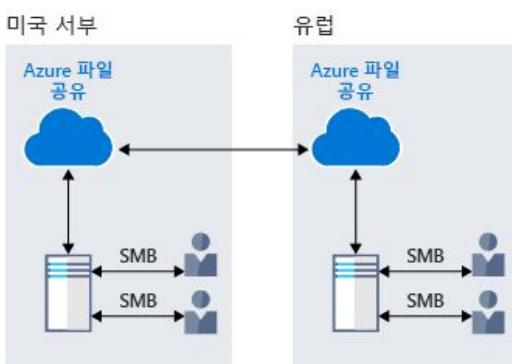
2. Azure Data Lake Storage

- 데이터 사용량을 분석하고 보고서를 준비하며, 구조적 데이터와 비정형 데이터가 모두 저장되는 대형 리포지토리이다
- 개체 스토리지의 확장성 및 비용 혜택이 빅 데이터 파일 시스템 기능의 안정성 및 성능과 결합되어 있다
- 아래의 그림은 Azure Data Lake가 모든 비즈니스 데이터를 저장하고 분석을 위해 제공하는 방식을 보여준다



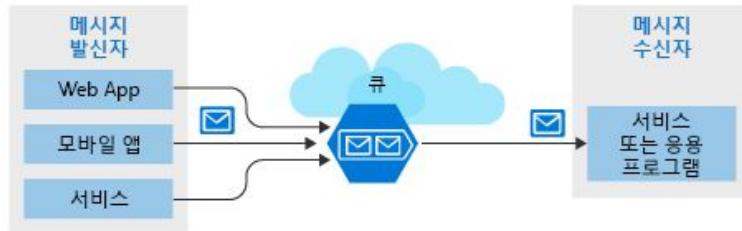
3. Azure Files

- 산업표준 SMB(서버 메시지 블록) 프로토콜을 통해 액세스 할 수 있는 완전 관리형 파일 공유를 제공한다
- Windows,Linux,macOS의 클라우드 또는 온-프레미스 배포를 통해 동시에 탑재 될 수 있다
- 가상머신 등 클라우드 환경에서 실행되는 애플리케이션은 데스크톱 애플리케이션이 일반적인 SMB 공유를 탑재하는 것처럼 File Storage 공유를 탑재하여 파일 데이터에 액세스 할 수 있다
- 무제한의 Azure VM 또는 억할이 파일 스토리지 공유를 동시에 탑재하고 액세스 할 수 있다
- 전 세계 어디서나 파일 공유가 가능하며, 진단 데이터 또는 애플리케이션 데이터를 공유하는 경우 사용한다
- 미사용 및 전송 중 데이터가 암호화되었는지 확인하는 SMB 프로토콜을 사용한다
- SMB를 통한 네트워크 드라이브 공유를 위한 스토리지



4. Azure Queue

- 전 세계 어디에서나 액세스 할 수 있는 많은 수의 메시지를 저장하기 위한 서비스
- 클라우드, 데스크톱, 온-프레미스, 모바일 디바이스에서 실행되는 애플리케이션 구성 요소 간의 통신을 위해 비동기식 메시지 대기열 기능을 제공한다
- 유연한 애플리케이션을 구축하고 기능을 분리하여 대용량 워크로드 전반에서 내구성을 향상 시킬 수 있다(애플리케이션 구성 요소가 분리되면 독립적인 확장이 가능하기 때문)
- 큐의 메시지를 추가하는 송신기, 큐의 앞에서 처리할 메시지를 검색하는 수신기가 하나 이상씩 구성 요소로 존재한다



큐 스토리지를 사용하여 다음을 수행할 수 있습니다.

- 작업의 백로그를 만들고 다른 Azure 웹 서버 간에 메시지를 전달합니다.
- 여러 웹 서버/인프라 간에 로드를 배포하고 트래픽 증가를 관리합니다.
- 여러 사용자가 동시에 데이터에 액세스할 때 구성 요소 오류에 대한 복원력을 빌드합니다.

5. Azure Disk Storage (Blob 스토리지에 저장)

- 가상 머신, 애플리케이션 및 기타 서비스가 액세스하여 사용 할 수 있는 디스크를 제공한다
- 데이터를 연결된 가상 하드 디스크에 영구적으로 저장 및 액세스 할 수 있게 한다
- Azure에서 관리하거나 관리하지 않을 수 있으므로 사용자가 관리하고 구성 할 수 있다
- 디스크는 SSD부터 기존의 회전식 하드 디스크 드라이브까지 다양한 크기와 성능 수준으로 제공한다
- VM을 사용할 때 덜 중요한 워크로드에는 표준SSD/HDD디스크를, 중요업무용 프로덕션 애플리케이션에는 프리미엄 SSD 디스크를 사용 할 수 있다
- 아래의 그림은 다른 데이터를 저장하기 위해 별도의 디스크를 사용하는 Azure VM이다



데이터베이스

- Azure에서는 다양한 형식과 볼륨의 데이터를 저장하도록 여러 DB 서비스를 제공한다
- 글로벌 연결을 통해 사용자는 이 데이터를 신속하게 받아서 사용할 수 있다

| 서비스 이름 | 서비스 기능 |
|----------------------------------|---|
| Azure Cosmos DB | NoSQL 옵션을 지원하는 글로벌 분산형 데이터베이스 |
| Azure SQL Database | 자동 크기 조정과 필수 인텔리전스, 강력한 보안을 통해 완벽하게 관리되는 관계형 데이터베이스입니다. |
| Azure Database for MySQL | 고가용성과 보안이 포함된 완벽하게 관리되고 확장 가능한 MySQL 관계형 데이터베이스 |
| Azure Database for PostgreSQL | 고가용성과 보안을 제공하며 완벽하게 관리되고 확장 가능한 PostgreSQL 관계형 데이터베이스입니다. |
| VM의 SQL Server | 클라우드에서 엔터프라이즈 SQL Server 앱 호스트 |
| Azure Synapse Analytics | 추가 비용 없이 모든 수준에서 필수 보안을 제공하며 완벽하게 관리되는 데이터 웨어하우스입니다. |
| Azure Database Migration Service | 애플리케이션 코드 변경 없이 클라우드로 데이터베이스를 마이그레이션합니다. |
| Azure Cache for Redis | 자주 사용하는 정적 데이터를 캐시하여 데이터 및 애플리케이션 대기 시간을 줄입니다. |
| Azure Database for MariaDB | 고가용성과 보안이 포함된 완벽하게 관리되고 확장 가능한 MariaDB 관계형 데이터베이스 |

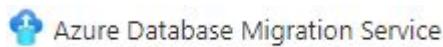
1. Azure SQL Database

- 최신 MS SQL Server 데이터베이스 엔진 버전을 기반으로 하는 관계형 DaaS(Database as a Service)
- 안정적이며, 안전하며 고성능을 제공하는 완전 관리형 데이터베이스이다
- 인프라를 따로 관리 할 필요 없이 선택한 프로그래밍 언어로 데이터 기반 애플리케이션 및 웹 사이트를 빌드하는 데 사용한다



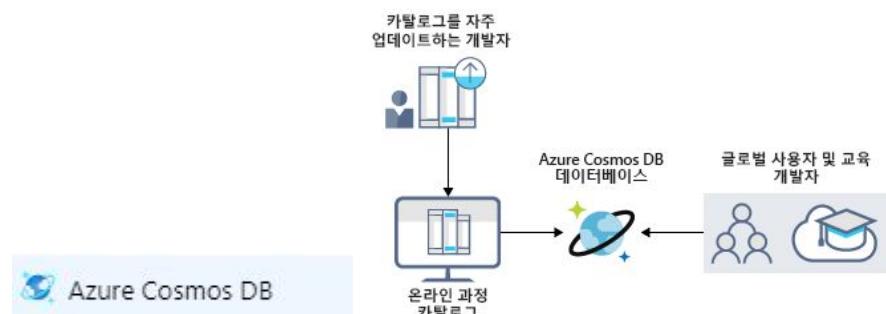
2. Azure Database Migration Service

- 최소한의 지연시간으로 기존의 SQL Server(온-프레미스)를 마이그레이션 할 수 있는 서비스
- Microsoft Data Migration Assistant를 사용하여 마이그레이션을 수행하기 전에 필요한 변경 사항을 설명하는 권장 사항을 제공하는 평가 보고서를 생성한다
- 필요한 수정을 평가하고, 마이그레이션을 시작 할 수 있다



3. Azure Cosmos DB

- 지속적으로 지원하기 위해 응답성이 뛰어난 Always On 애플리케이션을 빌드 할 수 있는 스키마 없는 데이터(NoSQL)를 지원하는 글로벌 분산형 데이터베이스 서비스이다.
- 해당 서비스를 사용하여 전세계 사용자가 업데이트하고 유지관리하는 데이터를 저장 할 수 있다
- 사용자는 모든 위치에서 데이터베이스를 투명하게 복제해서 사용할 수 있다



4. Azure cache for redis

- 오픈 소스 소프트웨어 Redis를 기반으로 하는 메모리 내 데이터 저장소를 제공하는 서비스
- 'Redis'는 백엔드 데이터 저장소에서 많이 사용하는 애플리케이션의 성능과 확장성을 개선한다
- 자주 액세스하는 데이터를 빠르게 쓰고 읽을 수 있는 서버 메모리에 보관하여 대량의 애플리케이션 요청을 처리 할 수 있다
- 'Redis'는 최신 애플리케이션에 매우 짧은 대기 시간 및 높은 처리량의 데이터 스토리지 솔루션을 제공한다
- Azure cache for redis는 Redis를 관리하는 서비스로 제공되고, 안전한 전용 Redis 서버 인스턴스와 전체 Redis API 호환성을 제공한다
- Azure 내부 또는 외부의 모든 애플리케이션에서 액세스 할 수 있다
- Azure cache for redis는 분산 데이터 또는 콘텐츠 캐시, 세션 저장소, 메시지 브로커 등으로 사용 할 수 있고, 독립 실행형으로 배포하거나 Azure SQL 또는 Cosmos DB와 같은 다른 Azure 데이터베이스 서비스와 함께 배포 할 수 있다
- Azure cache for redis는 Basic, Standard, Premium 계층에서 사용 할 수 있다

모바일

- Azure는 개발자가 iOS, Android, Windows 앱용 모바일 백엔드 서비스를 쉽고 빠르게 생성 할 수 있도록 한다
- 오프라인 데이터 동기화, 온프레미스 데이터 연결, 푸시 알림 브로드캐스트, 비즈니스 요구 사항과 일치하도록 자동 크기조정

API Management

개발자, 파트너 및 직원에게 안전하게 대규모로 API를 공유

App Service

강력한 웹 및 모바일용 클라우드 앱을 신속하게 구축

Azure Cognitive Search

모바일 앱 및 웹 앱 개발을 위한 AI 기반 클라우드 검색 서비스

Azure Maps

데이터에 지리적 컨텍스트를 제공하는 간단하고 안전한 위치 인식 API

Azure Cognitive Services

스마트 API 기능을 추가하여 상황에 맞는 상호 작용 가능

Notification Hubs

모든 백엔드에서 모든 종류의 플랫폼으로 푸시 알림을 전송할 수 있습니다.

Spatial Anchors

다중 사용자 공간 인식 혼합 현실 경험 만들기

Visual Studio App Center

지속적으로 모바일 및 데스크톱 앱 빌드, 테스트, 릴리스 및 모니터링

Xamarin

더 빠르게 클라우드 기반 모바일 앱 만들기

웹

- Azure에는 웹 앱 및 HTTP 기반 웹 서비스의 빌드 및 호스트에 대한 최고 수준의 자원이 포함되어 있다

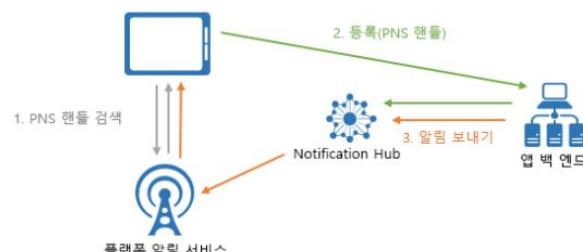
| 서비스 이름 | 설명 |
|--------------------------------|--|
| Azure App Service | 강력한 클라우드 웹 기반 앱을 신속하게 만들기 |
| Azure Notification Hubs | 원하는 백엔드에서 원하는 플랫폼으로 푸시 알림을 전송할 수 있습니다. |
| Azure API Management | 개발자, 파트너 및 직원에게 API를 안전하게 대규모로 공유할 수 있습니다. |
| Azure Cognitive Search | 완전 관리형 SaaS(Search-as-a-Service)입니다. |
| Azure App Service의 Web Apps 기능 | 중요 업무용 웹 앱을 대규모로 만들고 배포할 수 있습니다. |
| Azure SignalR Service | 실시간 웹 기능을 쉽게 추가할 수 있습니다. |

1. Azure App Service

- 웹 애플리케이션, REST API 및 모바일 백엔드를 호스트하는 HTTP 기반 서비스
- .NET, .NET Core, Java, Ruby, Node.js, PHP, Python 등 원하는 언어로 개발이 가능하고, Windows 및 Linux 기반 환경에서 애플리케이션을 쉽게 실행하고 확장 할 수 있다
- 보안, 부하분산, 자동 크기조정, 자동화된 관리의 기능을 애플리케이션에 추가한다
- Azure DevOps, GitHub, Docker 허브, 기타 원본, 패키지 관리, 스테이징 환경, 사용자 지정 도메인 및 TLS/SSL 인증서의 지속적인 배포와 같은 DevOps 기능도 활용 할 수 있다
- Azure 컴퓨팅 리소스에 대한 비용을 지불하게 된다
- 여러 언어 및 프레임워크, 관리형 프로덕션 환경(자동 패치 유지 관리), 컨테이너화 및 Docker, DevOps의 최적화, 고가용성을 가진 글로벌 규모 조정, SaaS 플랫폼 및 온프레미스 데이터에 연결, 보안 및 규정 준수, 애플리케이션 템플릿(MarketPlace), Visual Studio와 Visual Studio Code 통합, API 및 모바일 기능, 서비스 코드 등의 주요 기능

2. Azure Notification Hubs

- 알림을 모든 백엔드(클라우드 또는 온프레미스)에서 모든 플랫폼(iOS, Android, Windows...)으로 보낼 수 있는 간편하고 규모가 확장된 푸시 엔진을 제공하는 서비스
- 해당 서비스를 사용하면 백엔드에서 사용자 또는 관심 그룹에 메시지를 보내는 동안 디바이스는 PNS 핸들을 허브에 등록하는 역할만 수행하기 때문에 코딩을 줄이고 백엔드를 간소화하는 이점이 있다



3. Azure SignalR Service

- HTTP를 통해 애플리케이션에 실시간 웹 기능을 추가하는 프로세스를 간소화하는 서비스
- 실시간 기능을 사용하여 서비스가 연결된 클라이언트 콘텐츠 업데이트를 푸시 할 수 있다
- 클라이언트가 폴링하거나 업데이트에 대한 새 HTTP 요청을 제출하지 않고도 업데이트한다

Azure SignalR Service의 용도는?

- 높은 빈도 데이터 업데이트: 게임, 투표, 폴링, 경매
- 대시보드 및 모니터링: 회사 대시보드, 금융 시장 데이터, 인스턴트 판매 업데이트, 다중 플레이어 게임 리더 보드, IoT 모니터링
- 채팅: 라이브 채팅방, 채팅 봇, 온라인 고객 지원, 실시간 쇼핑 지원, 메신저, 인게임 채팅 등
- 지도의 실시간 위치: 물류 추적, 배달 상태 추적, 운송 상태 업데이트, GPS 앱
- 실시간 타겟팅 광고: 맞춤형 실시간 푸시 광고 및 제품, 대화형 광고.
- 협업 앱: 공동 작성, 화이트보드 앱, 팀 모임 소프트웨어
- 푸시 알림: 소셜 네트워크, 메일, 게임, 여행 경보
- 실시간 브로드캐스트: 라이브 오디오/비디오 브로드캐스트, 실시간 캡션, 번역, 이벤트/뉴스 브로드캐스트
- IoT 및 연결된 디바이스: 실시간 IoT 메트릭, 원격 제어, 실시간 상태, 위치 추적
- 자동화: 업스트림 이벤트의 실시간 트리거

사물인터넷 IoT

- Azure에서 IoT를 위한 엔드투엔드 솔루션을 지원하고 구동할 수 있는 여러 서비스가 존재한다

| 서비스 이름 | 설명 |
|---------------|---|
| IoT Central | 대규모 IoT 자산의 연결, 모니터링 및 관리를 도와주는, 완전히 관리되는 글로벌 IoT SaaS(Software-as-a-Service) 솔루션 |
| Azure IoT Hub | 수백만 개의 IoT 디바이스 간의 안전한 통신 및 모니터링을 제공하는 메시징 허브 |
| IoT Edge | 데이터 분석 모델을 IoT 디바이스로 직접 푸시하여 클라우드 기반 AI 모델을 참조할 필요 없이 상태 변경에 신속하게 대응할 수 있습니다. |

1. IoT Central

- 엔터프라이즈급 IoT 솔루션의 개발, 관리 및 유지 관리 부담과 비용을 줄이는 IoT 애플리케이션 플랫폼
- 복잡하고 지속적으로 진화하는 IoT 인프라를 단순히 유지 관리하는 것 뿐만 아니라 IoT 데이터를 활용하여 비즈니스를 전환하는데 시간,비용,에너지를 집중 할 수 있다
- 웹 UI를 통해 디바이스 상태를 모니터링하고, 규칙을 만들고, 전체 수명 주기 동안 수백만대의 디바이스와 해당 데이터를 관리 할 수 있다
- IoT 인텔리전스를 LOB(기간 업무) 애플리케이션으로 확장하여 디바이스 인사이트를 기반으로 조치를 취할 수 있다

2. Azure IoT Hub

- IoT 애플리케이션과 이를 통해 관리되는 디바이스 간의 양방향 통신을 위한 중앙 메시지 허브 역할
- 수백만개의 IoT 디바이스와 클라우드 호스팅 솔루션 백엔드 간에 안정적이고 안전한 통신을 통해 IoT 솔루션을 구축할 수 있음
- 수백만개의 센서(디바이스)에서 방대한 데이터를 제공
- Azure Blob Storage 및 Azure Data Lake Storage의 두 가지 스토리지 서비스로 메시지를 라우팅 할 수 있음

3. Azure IoT Hub DPS(Device Provisioning Service)

- IoT Hub용 도우미 서비스로, 사용자 개입 없이 적합한 IoT 허브에 자동 프로비저닝을 수행할 수 있는 서비스
- 수백만대의 디바이스를 확장 가능한 방식으로 안전하게 프로비저닝 할 수 있다
- 수백만개의 센서에서 데이터를 제공하여 Azure Data Lake에 저장

4. Azure IoT Edge

- 조직에서 데이터 관리 대신 비즈니스 통찰력에 집중할 수 있도록 클라우드 분석 및 사용자 지정 비즈니스 논리를 디바이스로 푸시한다
- 비즈니스 논리를 표준 컨테이너에 패키징하여 IoT 솔루션을 확장하면 모든 디바이스에 해당 컨테이너를 배포하고 클라우드에서 모든 컨테이너를 모니터링 할 수 있다
- 응급 상황에서 최대한 신속하게 대응하려면 Edge에서 변칙 검색 워크로드를 실행한다
- 대역폭 비용을 줄이고 대용량 원시 데이터를 전송하는 일이 없도록 하려면 로컬 데이터를 정리하고 집계한 다음, 인사이트만 클라우드로 보내서 분석하면 된다

Azure IoT Edge는 다음과 같은 세 가지 구성 요소로 구성됩니다.

- IoT Edge 모듈은 Azure 서비스, 타사 서비스 또는 개발자 고유의 코드를 실행하는 컨테이너입니다. 모듈은 IoT Edge 디바이스에 배포되어 해당 디바이스에서 로컬로 실행됩니다.
- IoT Edge 런타임은 각 IoT Edge 디바이스에서 실행되며 각 디바이스에 배포된 모듈을 관리합니다.
- 클라우드 기반 인터페이스를 사용하여 IoT Edge 디바이스를 원격으로 모니터링 및 관리할 수 있습니다.

AI

- Azure에서 가장 일반적인 AI 및 Machine Learning 서비스 유형을 지원한다

| 서비스 이름 | 설명 |
|-------------------------------|---|
| Azure Machine Learning 서비스 | 기계 학습 모델의 개발, 교육, 테스트, 배포, 관리 및 추적에 사용할 수 있는 클라우드 기반 환경입니다. 모델을 자동으로 생성하여 사용자에게 조정할 수 있습니다. 이를 사용하면 로컬 머신의 학습을 시작한 다음, 클라우드로 확장할 수 있습니다. |
| Azure Machine Learning Studio | 미리 빌드된 기계 학습 알고리즘 및 데이터 처리 모듈을 사용하여 기계 학습 솔루션을 빌드, 테스트, 배포할 수 있는 편리한 웹 기반 환경입니다. 다양한 기계 학습 모델과 함께 데이터 전처리, 모델 평가 및 배포 등 전통적인 기계 학습 단계를 지원합니다. |

1. Azure Machine Learning(미래동작, 결과 및 추세를 예측하는 데이터 과학 기술)

- 전통적인 기계 학습부터 딥러닝, 감독 학습 및 자율 학습에 이르는 모든 종류의 기계 학습에 사용할 수 있는 서비스
- SDK를 사용하여 Python 또는 R코드를 작성하든 스튜디오에서 코드 없음/낮은 코드 옵션으로 작업하든 상관없이 해당 서비스 영역에서 기계 학습 및 딥러닝 모델을 빌드, 학습 및 추적할 수 있다

2. Azure Machine Learning Studio

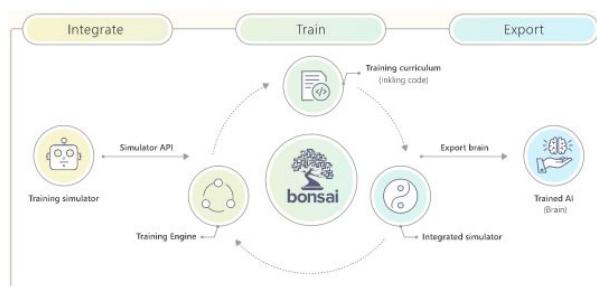
- 포괄적인 데이터 과학 플랫폼을 코드 없는 환경과 코드 우선 환경을 결합하는 웹 포털 서비스
- 형식 프로젝트와 사용자 환경 수준에 따라 여러 제작 환경을 제공한다
- 'Azure Machine Designer'를 사용하여 코드를 작성하지 않고도 기계 학습 모델을 학습하고 배포 할 수 있다
- 브라우저에서 직접 기계 학습 자산(모델, 데이터셋, 데이터저장소,Copute resource, Notebooks, 실험, 실험로그, Pipelines, 파이프라인 앤드포인트)을 관리하고, 원활한 환경을 위해 SDK와 스튜디오 간에 자산이 동일한 작업 영역에서 공된다

3. Azure Bot Service & Bot framework

- Intelligent bot을 한 곳에서 빌드, 테스트, 배포, 관리하는 도구를 제공하는 서비스
- Bot framework에는 bot, 도구, 템플릿, 관련 AI 서비스를 빌드하기 위한 모듈식 및 확장 가능한 SDK가 포함되어 있다
- 개발자는 이 프레임 워크를 사용하여 음성을 사용하고 자연어를 이해하고 질문 및 답변을 처리 할 수 있는 봇을 만들 수 있다

4. Azure Bonsai

- MS의 Autonomous Systems 제품군의 기계 교육 서비스
- 해당 서비스를 사용하여 복잡한 시스템을 제어하고 최적화하는 AI 모델(두뇌)을 생성한다
- 심층 강화 학습을 통해 기계 교육을 단순화하므로 보다 스마트한 자율 시스템을 교육하고 배포 할 수 있다



5. Cognitive Service

- REST API가 있는 클라우드 서비스이며, 개발자가 직접적인 AI(인공지능) 또는 데이터 과학 기술이나 지식 없이도 인지 지능형 애플리케이션을 빌드하는데 도움이 되도록 사용 할 수 있는 클라이언트 라이브러리 SDK이다
- 개발자가 보고, 듣고, 말하고, 이해하고, 추론까지 할 수 있는 애플리케이션을 만들도록 지원하는 목표를 갖고 있다
- 서비스 내 주요 카탈로그는 Vision, Speech, Language, Web Search, Decision이 있다

밀접한 관련이 있는 제품 세트를 _Cognitive Services_라고 합니다. 다음은 애플리케이션에서 복잡한 문제를 해결하는데 활용할 수 있는 미리 빌드된 API입니다.

| 서비스 이름 | 설명 |
|-------------|--|
| Vision | 사진과 동영상의 스마트한 식별, 캡션, 인덱싱, 종재를 수행하는 이미지 처리 알고리즘입니다. |
| Speech | 음성을 텍스트로 변환하거나, 음성을 인증에 사용하거나, 앱에 화자 인식을 추가하세요. |
| 지식 매팅 | 지능형 추천 및 의미 체계 검색 등의 작업을 해결하기 위해 복잡한 정보와 데이터를 매팅하세요. |
| Bing Search | Add Bing Search API를 앱에 추가하고 단일 API 호출 기능을 활용하여 수십억 개의 웹 페이지, 이미지, 동영상 및 뉴스를 철저히 검색하는 기능을 활용해 보세요. |
| 자연어 처리 | 미리 빌드된 스크립트를 사용하여 자연어를 처리하고, 감정을 평가하고, 사용자가 원하는 것을 인식하는 방법을 알아보세요. |

Azure DevOps *Dev(개발) + Ops(운영)

- Azure는 여러 도구와 기술을 제공하여 제품을 개발하는 동안 거의 모든 방법으로 조직에 도움이 되는 많은 서비스와 기능을 제공하는 클라우드 솔루션이다
- 웹 브라우저를 통해 액세스 할 수 있는 통합 기능 세트를 제공한다
- 리포지토리 및 애플리케이션 테스트를 통합, 애플리케이션 모니터링 수행, 빌드 아티팩트로 작업 할 수 있다.
- 추적용 백로그 항목으로 작업하고, 인프라 배포를 자동화하고, Jenkins 및 Chef와 같은 광범위한 타사 도구 및 서비스를 통합 할 수 있다

| 서비스 이름 | 설명 |
|--------------------|--|
| Azure DevOps | Azure DevOps Services(이전 명칭: Visual Studio Team Services 또는 VSTS)는 고성능 파이프라인, 무료 비공개 Git 리포지토리, 구성 가능한 Kanban 보드, 광범위한 자동 및 클라우드 기반 부하 테스트를 비롯한 개발 협업 도구를 제공합니다. |
| Azure DevTest Labs | 배포 파이프라인에서 바로 애플리케이션을 테스트하거나 시연하는 데 사용할 수 있는 주문형 Windows 및 Linux 환경을 신속하게 만듭니다. |

1. Azure DevTest lab

- Azure DevTest labs를 통해 개발자는 관리자의 승인을 기다리지 않고 가상머신 및 PaaS 리소스를 효율적으로 자체 관리 할 수 있다
- 환경을 만드는데 사용할 수 있는 필요한 모든 도구와 소프트웨어가 포함된 기본 템플릿 또는 Azure Resource Manager 템플릿으로 구성된 랙을 생성하여 몇분 내에 환경을 구성 할 수 있다
- 재사용 가능한 템플릿 및 아티팩트를 사용하여 Windows 및 Linux 환경을 신속하게 프로비저닝 할 수 있다
- 배포 파이프라인과 DevTest Lab을 쉽게 통합하여 주문형 환경으로 프로비저닝 할 수 있다
- 여러 테스트 에이전트를 프로비저닝하여 부하 테스트를 강화하고 교육 및 데모를 위해 미리 프로비저닝된 환경을 만들 수 있다

2. Azure Repos

- 코드를 관리하는 데 사용 할 수 있는 버전 관리 도구의 집합
- 버전 제어 시스템은 시간 경과에 따른 코드 변경사항을 추적하는데 도움이 되는 소프트웨어(Git..)
- 코드를 편집 할 때 버전 제어 시스템에 파일의 스냅샷을 사용하도록 지시한다
- 버전 제어 시스템은 해당 스냅샷을 영구적으로 저장하므로 나중에 필요할 때 다시 불러올 수 있다
- 단일 개발자라도 버전제어를 사용하면 버그를 수정하고 새로운 기능을 개발할 때 체계적으로 유지 할 수 있는 장점이 있다

3. 기타 DevOps 서비스

Azure Artifacts

패키지를 만들고 호스트한 후 팀과 공유

Azure DevOps

팀 간의 코드 공유, 작업 추적 및 소프트웨어 전송을 위한 서비스

Azure Monitor

애플리케이션, 인프라 및 네트워크에 대한 포괄적인 운영 가시성

Azure Repos

프로젝트에 적합한 무제한 클라우드 기반 개인 Git 리포지토리 사용

DevOps Tool Integrations

Azure에서 선호하는 DevOps 도구 사용

Azure Boards

팀에서 작업 계획, 추적 및 논의

Azure DevTest Lab

재사용 가능한 템플릿 및 아티팩트를 사용하는 환경을 신속하게 조성

Azure Pipelines

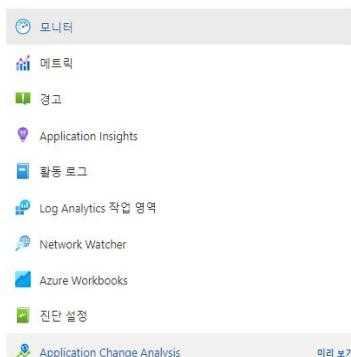
모든 플랫폼 및 클라우드에 지속적으로 빌드, 테스트 및 배포

Azure Test Plans

매뉴얼 및 예비 테스트 도구 키트로 안심하고 테스트 및 제공

Azure Monitor

- 클라우드 및 온프레미스 환경에서 원격 분석 데이터를 수집, 분석하고 그에 따라 조치를 취하는 포괄적인 솔루션을 제공함으로써 애플리케이션 및 서비스의 성능과 가용성을 최대화한다



- 애플리케이션을 수행하는 방법과 애플리케이션 및 종속된 리소스에 영향을 주는 문제를 사전에 식별하여 예방 할 수 있다
- Application Insights를 사용하여 애플리케이션 및 종속성 간의 문제를 감지하고 진단한다
- 인프라문제를 VM용 Azure Monitor과 컨테이너용을 상호연결하여 문제를 식별한다
- 문제 해결 및 심층진단을 위해 Log Analytics를 사용하여 모니터링 데이터를 받는다
- 스마트 경고 및 자동작업을 사용하여 규모에 맞게 작업을 지원한다

Azure 대시보드 및 통합문서를 사용하여 시각화한다

1. Application Insights

- 개발자 및 DevOps 전문가를 위한 확장 가능한 APM(애플리케이션 성능관리)서비스
- 실행중인 애플리케이션을 모니터링하는데 사용한다
- 성능 이상을 감지하고, 문제를 진단하고 사용자가 사용하는 앱의 수행하는 작업을 파악 할 수 있는 강력한 분석도구를 가지고 있다
- 성능 및 고가용성을 지속적으로 항상 시킬 수 있도록 설계한다
- DevOps 프로세스와 통합되며, 다양한 개발 도구와의 연결지점을 갖고 있다

2. Azure Log Analytics

- 로그 쿼리를 작성하고 대화형으로 결과를 분석하기 위한 기본 도구
- 로그 쿼리는 다른 리소스에서도 사용되지만, 일반적으로 Log Analytics를 사용하여 쿼리를 작성하고 테스트한다
- Log Analytics는 Azure Portal 여러 위치에서 사용이 가능하다
ex. VM을 특정기간동안 켜거나 끈 log

3. VM용 Azure Monitor

- 실행중인 프로세스 및 다른 리소스에 대한 종속성을 포함하여 가상머신 및 가상머신 확장집합의 성능 및 상태를 모니터링한다
- 성능 병목현상 및 네트워크 문제를 식별하여 중요한 응용 프로그램의 예측 가능한 성능 및 가용성을 제공할 수 있으며 문제가 다른 종속성과 관련되어 있는지 여부를 파악할 수도 있다
- 해당 기능은 Windows 및 Linux 운영 체제를 지원한다
- 수집한 데이터를 Azure Monitor 로그에 저장하고, 이를 통해 강력한 집계 및 필터링을 제공하고 시간에 따른 데이터 추세를 분석한다

4. Azure Network Watcher

- Azure 가상 네트워크의 리소스를 모니터링 및 진단하고 메트릭을 보고 그에 대한 로그를 활성화 또는 비활성화하는 도구를 제공한다
- Virtual Machines, Virtual Networks, Application Gateways, 부하 분산 장치 등을 포함하는 IaaS 제품의 네트워크 상태를 모니터링하고 복구하도록 설계되었다

5. Azure Application Change Analysis (응용 프로그램 변경 분석)

- 데이터 원본의 변경 데이터를 계산하고 집계하고, 사용자가 모든 리소스 변경사항을 쉽게 탐색하고 문제해결 또는 모니터링 상황과 관련된 변경내용을 식별할 수 있도록 분석 집합을 제공한다

- 해당 서비스의 리소스 공급자는 Azure Resource Manager 추적 속성 및 프록시 설정 변경 데이터를 사용할 수 있도록 구독에 등록해야 한다
- 웹앱에 대한 변경 분석을 사용하도록 설정 하는 경우 웹앱에 대한 성능 영향을 최소화 하고 청구 비용을 부과하지 않는다
- Azure Monitor에는 응용 프로그램 종속성 및 리소스에 대한 정보를 포함하는 모든 변경 내용을 볼 수 있는 득립 실행형 창이 있다

6. Azure service Health

- Azure 서비스 관련 문제가 사용자에게 영향을 주는 경우 맞춤형 지침과 지원을 제공하는 환경의 도구모음
- 사용자에게 알리고, 문제의 영향을 이해할 수 있도록 지원하고, 문제가 해결되는대로 계속 업데이트 할 수 있고, 리소스의 가용성에 영향을 줄 수 있는 계획된 유지 관리 및 변경내용을 준비하는데 도움이 된다
- Azure 환경에 배포된 모든 서비스와 사용 할 수 있는 모든 서비스의 상태를 볼 수 있으며, 서비스가 실패할 경우 경고를 받는 규칙을 생성 가능하다

Azure 상태는 Azure 서비스의 상태에 대한 글로벌 보기¹를 제공합니다. Azure 상태를 사용하여 서비스 가용성에 대한 최신 정보를 얻을 수 있습니다. 모든 사용자는 Azure 상태에 액세스할 수 있으며 해당 상태를 보고하는 모든 서비스를 볼 수 있습니다.

Service Health는 사용하는 영역에 있는 Azure 서비스를 사용하는 지역에서 해당 상태를 추적하는 사용자 지정 가능한 대시보드를 제공합니다. 이 대시보드에서는 지속적인 서비스 문제, 계획된 향후 유지 관리 또는 관련 상태 공지와 같은 활성 이벤트를 추적할 수 있습니다. 비활성화 된 이벤트는 최대 90일 동안 상태 기록에 저장됩니다. 마지막으로 Service Health 대시보드를 사용하여 사용자에게 영향을 주는 서비스 문제가 있을 때마다 알려주는 서비스 상태 경고를 만들고 관리할 수 있습니다.

Resource Health를 사용하면 Azure 서비스 문제²가 리소스에 영향을 줄 때 이를 진단하고 지원을 받을 수 있습니다. 리소스의 현재 및 과거 상태에 대한 자세한 정보를 제공합니다. 또한 문제를 완화하는 데 도움이 되는 기술 지원을 제공합니다. 일단의 광범위한 Azure 고객에게 영향을 주는 서비스 문제를 알려주는 Azure 상태와 달리, Resource Health는 리소스의 상태에 대한 맞춤형 대시보드를 제공합니다. Resource Health는 과거 Azure 서비스 문제로 인해 리소스를 사용할 수 없었던 시간을 보여 줍니다. 따라서 SLA가 위반되었는지 쉽게 파악할 수 있습니다.

전체적으로 Azure Service Health 구성 요소는 가장 관련성이 높은 세분화 수준에서 Azure의 상태에 대한 포괄적인 보기를 제공합니다.

Azure 분석 서비스

- 분석 서비스를 통해 전체 데이터 자산을 사용하여 엔터프라이즈 규모에서 혁신적이고 안전한 분석 솔루션을 빌드 할 수 있다
- Azure Data Lake Storage Gen2, Data Factory, Databricks, Azure Synapse Analytics 등의 완전 관리형 서비스를 통해 BI(Business Intelligence) 및 보고, 고급 분석 및 실시간 분석을 위한 솔루션을 쉽게 배포할 수 있다
- 조직의 모든 사용자를 위한 뛰어난 Power BI 시각화를 통해 데이터를 시기적절한 분석으로 변환한다

인사이트를 가장 빠르게 얻을 수 있는 무제한 분석 서비스(이전의 SQL Data Warehouse) [Azure Synapse Analytics](#)

Azure에 최적화된 빠르고 쉽게 협업이 가능한 완전관리형 Apache® Spark™ 기반 분석 플랫폼 [Azure Databricks](#)

99.9% SLA를 보장하는 기업용 완전 관리형 클라우드 Hadoop 및 Spark 서비스 [HDInsight](#)

데이터 이동 및 변환을 오케스트레이션 및 자동화하는 데이터 통합 서비스 [Data Factory](#)

클라우드 및 에지를 포괄하는 개방형의 탄력적 AI 개발 [머신 러닝](#)

수백만 개의 IoT 디바이스에서 실시간 데이터 스트림 처리 [Azure Stream Analytics](#)

엔터프라이즈급 보안, 감사 및 지원이 포함된 완전 관리, 주문형 유료 분석 서비스 [Data Lake Analytics](#)

엔터프라이즈급 분석 엔진을 서비스로 제공 [Azure Analysis Services](#)

수백만 개의 이벤트를 수집, 변환 및 저장하는 하이퍼스케일(hyper-scale) 원격 분석 수집 서비스 [Event Hubs](#)

빠르고 확장성이 뛰어난 데이터 탐색 서비스 [Azure Data Explorer](#)

외부 조직과 빅 데이터를 안전하고 간단하게 공유할 수 있는 서비스입니다. [Azure Data Share](#)

대규모 산업용 IoT 데이터를 모니터링, 분석 및 시각화하는 엔드투엔드 IoT 분석 플랫폼 [Azure Time Series Insights](#)

1. Azure HDInsight

- 클라우드의 관리형 전체 스펙트럼 오픈 소스 프레임워크(Hadoop)를 사용하여 대량의 데이터 분석/처리 서비스
- 2. Azure Synapse Analytics(SQL Data Warehouse + Data Lake Analytics)**
- 데이터 웨어하우징과 빅데이터 분석을 결합한 분석서비스
- 서비스 주문형 리소스 또는 프로비저닝된 리소스를 규모에 맞게 사용하여 사용자의 용어로 데이터를 자유롭게 쿼리 할 수 있다
- 즉각적인 요구에 따라 데이터를 수집, 준비, 관리 할 수 있다

Azure Synapse에는 다음 네 가지 구성 요소가 있습니다.

- Synapse SQL: 전체 T-SQL 기반 분석 – 일반 공급
 - SQL 풀(프로비저닝되는 DWU당 요금 지불)
 - SQL 주문형(처리되는 TB당 요금 지불)(미리 보기)
- Spark: 긴밀하게 통합된 Apache Spark(미리 보기)
- Synapse 파이프라인: 하이브리드 데이터 통합(미리 보기)
- 스튜디오: 통합 사용자 환경. (미리 보기)

3. Azure Databricks

- Azure 클라우드 플랫폼에 대해 최적화된 Apache Spark 기반 분석 플랫폼이다 (Apache Spark란 빅데이터처리를 위한 오픈소스 병렬분산처리 플랫폼이다)
- 원클릭 설정, 간소화된 워크플로 및 데이터 과학자, 데이터 엔지니어, 비즈니스 분석가가 협업할 수 있도록 하는 대화형 작업 영역을 제공한다



4. Azure Data Factory

- 빅데이터는 원시데이터(관계형,비관계형)와는 다르게 수많은 원시 데이터 저장소를 조치 가능한 비즈니스 통찰력으로 구체화하도록 프로세스를 조율하고 운영할 수 있는 서비스가 필요하다
- 복잡한 하이브리드 ETL(추출-변환-로드) ELT(추출-로드-변환) 및 데이터 통합 프로젝트를 위해 만들어진 관리되는 클라우드 서비스
- 인사이트(통찰력)를 추출하기 위해 Spark 클러스터를 사용하여 조인한 데이터를 처리하고(Azure HDInsight), 변환된 데이터를 Azure Synapse Analytics와 같은 클라우드 데이터 웨어하우스에 게시하여 데이터를 바탕으로 보고서를 쉽게 작성하려고 하고, 이 워크플로를 자동화하고 일일 일정으로 모니터링 및 관리하려고 한다. 또한 파일이 Blob 저장소 컨테이너에 배치 될 때 실행하려고 하는데, 이를 해결하는 플랫폼이 Data Factory이다

5. Azure Stream Analytics

- 여러 원본에서 대량의 빠른 스트리밍 데이터를 동시에 분석 및 처리하도록 설계된 실시간 분석 및 복잡한 이벤트 처리엔진
- 패턴과 관계는 디바이스, 센서, 클릭스트림, 소셜 미디어 피드 및 애플리케이션을 포함한 여러 입력 원본에서 추출한 정보에서 식별할 수 있다
- 이러한 패턴을 사용하여 경고를 만들거나, 보고 도구에 정보를 공급하거나, 나중에 사용할 수 있도록 변환된 데이터를 저장하는 등의 작업을 트리거하고 워크플로를 시작할 수 있다
- 해당 서비스는 Azure IoT Edge 런타임에서 사용할 수 있으며, IoT 디바이스에서 데이터를 처리 할 수 있다

다음 시나리오는 Azure Stream Analytics를 사용할 수 있는 경우의 예입니다.

- IoT 디바이스에서 실시간 원격 분석 스트림 분석
- 웹 로그/클릭 스트림 분석
- fleet 관리 및 드라이버가 없는 자동차에 대한 지리 공간적 분석
- 원격 모니터링 및 높은 가치 자산의 예측 유지 관리
- 인벤토리 제어 및 변칙 검색에 대한 판매 시점 데이터에 대한 실시간 분석

6. Azure Event Hubs

- 동적 데이터 파이프라인을 통해 초당 수백만개의 실시간 데이터 이벤트를 수신하고 처리 할 수 있는 빅데이터 스트리밍 플랫폼 및 이벤트 수집 서비스
- Event Hub로 전송된 데이터는 실시간 분석 공급자 또는 일괄처리/스토리지 어댑터를 사용하여 변환하고 저장할 수 있다
- 다른 Azure 서비스와도 원활하게 통합될 수 있다
- 구성 또는 관리 오버헤드가 거의 없는 완전관리형 PaaS으로 사용자가 비즈니스 솔루션에 집중 할 수 있다

Azure Migration

- 온프레미스 서버, 인프라, 애플리케이션 및 데이터를 평가하고 Azure로 마이그레이션 할 수 있는 중앙 허브를 제공한다

| 도구 | 평가 및 마이그레이션 | 세부 정보 |
|----------------------------------|---|--|
| Azure Migrate: Server Assessment | 서버를 평가합니다. | Azure로 마이그레이션하기 위한 준비 과정으로 온-프레미스 VMware VM, Hyper-V VM 및 물리적 서버를 검색하고 평가합니다. |
| Azure Migrate: Server Migration | 서버를 마이그레이션합니다. | VMware VM, Hyper-V VM, 물리적 서버, 기타 가상화된 머신 및 퍼블릭 클라우드 VM을 Azure로 마이그레이션합니다. |
| 데이터 Migration Assistant | Azure SQL Database, Azure SQL Managed Instance 또는 SQL Server를 실행하는 Azure VM으로 마이그레이션할 SQL Server 데이터베이스를 평가합니다. | Data Migration Assistant는 마이그레이션을 자단하는 잠재적인 문제를 파악하는 데 도움이 됩니다. 이는 지원되지 않는 기능, 마이그레이션 후 유용할 수 있는 새로운 기능, 데이터베이스 마이그레이션의 올바른 경로를 식별합니다. 자세히 알아보기. |
| Azure Database Migration Service | 온-프레미스 데이터베이스를 SQL Server, Azure SQL Database 또는 SQL Managed Instance를 실행하는 Azure VM으로 마이그레이션합니다. | Database Migration Service에 대해 자세히 알아보기 |
| Movere | 서버를 평가합니다. | Movere에 대해 자세히 알아보세요. |
| Web App Migration Assistant | 온-프레미스 웹 앱을 평가하고 Azure로 마이그레이션합니다. | Azure App Service Migration Assistant를 사용하여 Azure App Service으로 마이그레이션하기 위한 온-프레미스 웹 사이트를 평가합니다. 이 Migration Assistant를 사용하여 .NET 및 PHP 웹 앱을 Azure로 마이그레이션합니다. Azure App Service Migration Assistant에 대해 자세히 알아보세요. |
| Azure Data Box | 오프라인 데이터를 마이그레이션합니다. | Azure Data Box 제품을 사용하여 대량의 오프라인 데이터를 Azure로 이동합니다. 자세히 알아보기. |

기타 서비스

1. Azure Blockchain Service

- 사용자가 Azure에서 대규모로 Blockchain 네트워크를 확장하고 작동할 수 있도록 하는 완전 관리형 원장 서비스
- 네트워크 거버넌스 뿐만 아니라 인프라 관리를 통합적으로 제어하여 간단한 네트워크 배포 및 작업, 기본 제공 컨소시엄 관리, 친숙한 개발 도구를 사용하여 스마트 계약 개발 등의 기능을 제공함
- IBFT 합의 메커니즘을 사용하여 Ethereum Quorum 원장을 지원한다
- 가상머신과 인프라를 관리하는데 시간과 리소스를 할당하는 대신, 앱 개발 및 비즈니스 논리에 집중할 수 있다
- 새로운 기술을 습득하지 않고도 원하는 오픈소스 도구와 플랫폼을 사용하여 솔루션을 전달할 수 있는 애플리케이션을 계속 개발할 수 있다

보안, 개인정보 보호, 규정 준수 및 신뢰 설명

클라우드에서의 보안

- 컴퓨팅 환경이 고객제어 데이터센터(온프레미스)에서 클라우드로 전환되면서 보안의 책임소재가 클라우드 공급자와 고객 모두의 문제로 변화하였다
- 특정 서비스는 보안 기능을 기본 제공하여 고객에게 좀 더 개발에 매진할 수 있도록 하였고, 나머지 문제 해결의 책임은 고객이 지도록 하여, 적절한 보안제어가 이루어지도록 하고 있다

<각 클라우드 서비스의 보안>

- 모든 클라우드 배포유형에서의 사용자는 고유의 데이터와 ID를 소유한다
 - 배포유형과 관계없이 '데이터, 앤드포인트, 계정, 액세스관리'에 대한 책임은 항상 사용자에게 있다
1. **IaaS (Infrastructure as a Service)**
 - 이 계층에서는 여전히 운영 체제와 소프트웨어를 패치 및 보호하고 네트워크를 안전하게 유지하는 일은 사용자의 몫이다
 - Azure VM을 사용 할 때 운영상의 이점 외에도 네트워크의 물리적 부분을 보호하는 것과 관련하여 문제를 아웃소싱하는 보안상의 이점도 얻을 수 있다
 2. **PaaS (Platform as a Service)**
 - PaaS로의 이전은 여러 가지 보안 문제를 아웃소싱한다
 - 모든 소프트웨어는 최신 보안 패치로 업데이트되며, 액세스 제어를 위해 Azure AD와 통합 할 수 있다
 - 사용자 환경에 맞게 전체 인프라와 서브넷을 직접 빌드하는 대신, Azure Portal이나 자동화된 스크립트를 실행하여 복잡한 보안 시스템을 위아래로 이동하고 필요에 따라 크기를 조정 할 수 있다
 3. **SaaS (Software as a Service)**
 - SaaS를 사용하면 거의 모든 요소를 아웃소싱 할 수 있다
 - SaaS는 인터넷 인프라와 함께 실행되는 소프트웨어로, 코드는 공급업체가 제어하지만 고객이 사용하도록 구성된다

| Responsibility | On-prem | IaaS | PaaS | SaaS |
|-------------------------------------|---------|------|------|------|
| Data governance & rights management | ■ | ■ | ■ | ■ |
| Client endpoints | ■ | ■ | ■ | ■ |
| Account & access management | ■ | ■ | ■ | ■ |
| Identity & directory infrastructure | ■ | ■ | ■ | ■ |
| Application | ■ | ■ | ■ | ■ |
| Network controls | ■ | ■ | ■ | ■ |
| Operating system | ■ | ■ | ■ | ■ |
| Physical hosts | ■ | ■ | ■ | ■ |
| Physical network | ■ | ■ | ■ | ■ |
| Physical datacenter | ■ | ■ | ■ | ■ |

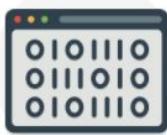
■ Microsoft ■ Customer

<보안에 대한 계층화된 접근 방법> 심층방어

- 심층방어는 정보에 무단으로 액세스하려는 공격의 진행 속도를 늦추는 일련의 메커니즘을 사용하는 전략이다
- 각 레이어가 보호를 제공하므로 한 레이어에서 보안 위반이 발생하더라도 후속 레이어가 이미 적용되어 추가 노출을 방지한다



데이터



대부분의 경우 공격자는 다음과 같은 데이터를 목표로 합니다.

- 데이터베이스에 저장된 데이터
- 가상 머신 내부의 디스크에 저장된 데이터
- Microsoft 365와 같은 SaaS 애플리케이션에 저장된 데이터
- 클라우드 스토리지에 저장된 데이터

데이터를 저장하고 액세스를 제어하는 사용자는 데이터를 적절하게 보호할 책임이 있습니다. 종종 데이터의 기밀성, 무결성 및 가용성을 보장하기 위한 제어 및 프로세스를 적용할 것을 지시하는 규제 요구 사항이 있습니다.

애플리케이션



- 애플리케이션이 안전하고 취약하지 않은지 확인합니다.

- 중요한 애플리케이션 비밀을 안전한 저장 매체에 저장하세요.

- 보안 항목을 모든 애플리케이션 개발의 디자인 요구사항에 포함합니다.

애플리케이션 개발 수명 주기에 보안을 통합하면 코드의 취약점을 줄일 수 있습니다. 모든 개발팀이 애플리케이션의 보안을 가장 기본으로 여기며 어떠한 경우에도 보안을 포기하지 않도록 권장합니다.

컴퓨팅



- 가상 머신에 대한 액세스를 보호합니다.

- 엔드포인트 보호를 구현하고 시스템을 패치하고 최신 상태로 유지합니다.

맬웨어, 패치되지 않은 시스템과 부적절한 보안 시스템은 사용자의 환경을 공격에 노출시킵니다. 이 레이어의 핵심은 컴퓨팅 리소스를 안전하게 보호하고 보안 문제를 최소화하는 적절한 제어가 마련되는 것입니다.

네트워킹



- 리소스 간의 통신을 제한합니다.

- 기본적으로 거부합니다.

- 적절한 경우 인바운드 인터넷 액세스를 금지하고 아웃바운드를 제한합니다.

- 온-프레미스 네트워크에 대한 보안 연결을 구현합니다.

이 레이어의 핵심은 모든 리소스에 대한 네트워크 연결을 제한하여 필요한 것만 허용합니다. 이 통신을 제한하여 네트워크 전체에서 횡적 이동의 위험을 줄입니다.

경계



- DDoS(분산 서비스 거부) 보호 기능을 사용하여 최종 사용자에게 서비스 거부가 발생하기 전에 대규모 공격을 필터링합니다.

- 경계 방화벽을 사용하여 네트워크에 대한 악의적인 공격을 식별하고 경고합니다.

네트워크 경계에서, 리소스에 대한 네트워크 기반 공격을 방어합니다. 이러한 공격을 파악하여 영향을 제거하고 발생한 공격을 경고하는 것이 네트워크를 안전하게 유지하는 중요한 방법입니다.

ID 및 액세스



- 인프라에 대한 접근 및 제어 변경을 통제합니다.

- Single Sign-On 및 다단계 인증을 사용합니다.

- 이벤트 및 변경 내용을 감사합니다.

ID 및 액세스 레이어는 ID를 안전하게 보호하고, 필요한 것에만 액세스 권한을 부여하고, 변경 내용을 기록하는지 확인합니다.

물리적 보안



- 물리적 빌딩 보안 및 데이터 센터 내의 컴퓨팅 하드웨어에 대한 액세스 제어가 첫 번째 방어선입니다.

물리적 보안을 사용하는 목적은 자산 액세스에 대한 물리적 보호 수단을 제공하는 것입니다. 이 보호 수단은 다른 레이어가 무시되지 않고 손실 또는 도난이 적절하게 처리되도록 합니다.

Azure Security Center

- Azure과 온프레미스 모든 서비스에 대한 위협 보호를 제공하는 모니터링 서비스
- 구성, 리소스 및 네트워크를 기반으로 보안 추천을 제공한다
- 온프레미스 및 클라우드 워크로드의 보안설정을 모니터링하면서 새 서비스가 온라인으로 전환되면 필요한 보안을 자동으로 적용한다
- 모든 서비스를 지속적으로 모니터링하면서 자동 보안 평가를 수행하여 잠재적 취약점이 악용되기전에 미리 식별한다
- 기계학습을 통하여 멀웨어를 탐지하고 가상머신과 서비스에 설치되지 않도록 차단하고, 유효성을 검사한 앱만 실행 할 수 있도록 허용되는 애플리케이션 목록을 정의 할 수 있다
- 잠재적 인바운드 공격을 분석 및 식별하고, 발생했을지도 모르는 위협 및 계시를 보안 위반 활동을 조사한다
- 포트에 대한 Just-in-Time(제시간에) 액세스 제어를 제공하고, 필요한 트래픽만 네트워크에서 허용하여 공격 노출 영역을 줄인다

<사용 가능 계층>

- 서비스의 전체 제품군에 액세스하려면 표준 계층 구독으로 업그레이드 해야한다
- 1. 체험 : Azure 구독의 일부로 제공되며, Azure 리소스의 평가 및 추천으로 제한한다
- 2. 표준 : 연속 모니터링, 위협탐지, 포트에 대한 액세스 제어를 포함하여 완전한 보안 관련 서비스 제품군을 제공한다

<Advisor과의 차이>

===== # ID 및 액세스 =====

- ID 및 액세스 제어의 기본적인 개념은 인증과 권한부여이다
- 인증과 권한부여는 발생하는 모든 것의 기반이 되며 ID 및 액세스 프로세스에서 순차적으로 이루어진다
- ‘인증’은 리소스에 액세스하려는 사람 또는 서비스의 ID를 설정하는 프로세스이다. 당사자에게 합법적인 자격증명을 요구하는 행동이 포함되며, ID 및 액세스 제어에 사용할 보안 주체를 만들기 위한 기반을 제공한다
- ‘권한부여’는 인증된 사용자 또는 서비스가 갖는 액세스 수준을 설정하는 프로세스이다. 액세스 할 수 있는 데이터와 해당 데이터로 할 수 있는 작업을 지정한다

<SSO> Single Sign-On

- 사용자가 ID 하나와 암호 하나만 기억하면 되고, 애플리케이션에 대한 액세스 권한이 사용자와 연결된 ID에 부여되므로 보안 모델이 간소화된다
- 액세스 수정이 단일 ID에 연결되어 있으므로 사용자 역할이 변경되거나 사용자가 조직을 떠날 때 계정을 변경하거나 비활성화 하는 과정이 대폭 축소된다

<다단계 인증> MFA

- 전체 인증에 2개 이상의 요소를 요구하여 ID에 추가 보안을 제공하는 기능이다

사용자가 알고 있는 것은 암호이거나 보안 질문에 대한 대답입니다. 사용자가 소유하고 있는 것은 알림을 받는 모바일 앱 또는 토큰 생성 디바이스일 수 있습니다. 사용자의 신원 정보는 여러 모바일 디바이스에서 사용되는 지문 또는 얼굴 검사처럼 일반적으로 생체 인식 속성의 일종입니다.

<역할 기반 액세스 제어> RBAC

- “읽기전용” “기여자”처럼 Azure 서비스 인스턴스에 액세스하도록 사용자에게 부여될 수 있는 권한 집합이다
- ID는 사용자에게 직접 부여하거나 그룹 멤버 자격을 통해 상속된다. 보안주체, 액세스 권한 및 리소스를 분리하면 액세스를 쉽게 관리하고 자세히 제어 할 수 있다
- 역할은 개별 서비스 인스턴스 수준에서 부여할 수 있지만 Azure Resource Manager 계층 구조를 따라 아래로 상속되기도 한다



<서비스에 ID 제공>

- 종종 자격증명 정보가 구성파일에 포함되는 경우가 있는데, 이러한 구성 파일과 관련된 보안이 전혀 없기 때문에 시스템 또는 리포지토리에 대한 액세스 권한을 부여한다

서비스 주체



서비스 주체를 이해하려면 ID 및 주체라는 단어가 ID 관리에 사용되는 방법 때문에 먼저 두 단어를 이해하는 것이 좋습니다.

ID는 인증 가능한 것을 의미합니다. 당연히 여기에는 사용자 이름 및 암호를 사용하는 사용자가 포함되지만, 비밀 키 또는 인증서를 사용하여 인증되는 애플리케이션 또는 다른 서버도 포함될 수 있습니다.

보안 주체는 특정 역할 또는 클레임을 사용하여 작동하는 ID입니다. 일반적으로 ID와 주체를 동일한 것으로 생각해도 별 무리가 없지만, Linux의 Bash 프롬프트에서 'sudo'를 사용하거나 Windows에서 "관리자 권한으로 실행"을 사용하는 경우를 생각해 봅시다. 위의 두 가지 경우에, 모두 이전과 같은 ID로 계속 로그인되지만, 실행하는 역할은 변경했습니다. 그룹은 권한을 할당받을 수 있으므로 주체로 간주되기도 합니다.

서비스 주체는 서비스 또는 애플리케이션에서 사용하는 ID를 말합니다. 다른 ID와 마찬가지로 서비스 주체는 할당된 역할일 수 있습니다.

Azure 서비스에 대한 관리형 ID



서비스 주체 만들기는 지루한 과정일 수 있으며 수많은 접점이 있어서 유지 관리가 어려울 수 있습니다. Azure 서비스의 관리 ID는 훨씬 간단하며 대부분의 작업을 자동으로 처리합니다.

관리 ID는 지원되는 모든 Azure 서비스에 대해 즉시 만들 수 있으며 그 수가 계속해서 늘고 있습니다. 특정 서비스의 관리 ID를 만들면 조직의 Active Directory에 계정이 만들어집니다(특정 조직의 Active Directory 인스턴스를 "Active Directory 테넌트"라고 함). Azure 인프라는 서비스를 인증하고 계정을 관리하는 작업을 자동으로 처리합니다. 그러면 사용자는 인증된 서비스가 다른 Azure 리소스에 안전하게 액세스하도록 허용하는 등 해당 계정을 다른 Azure AD 계정처럼 사용할 수 있습니다.

Azure Active Directory(AAD)

- 클라우드 기반 ID 및 액세스 관리 솔루션으로, 내부/외부/고객 ID를 보호하는데 유용하다
- 회사 내부 사용자에게 다른 Azure 서비스, Microsoft 365 및 타사 SaaS 애플리케이션과 같은 외부 리소스에 액세스하거나 회사 네트워크의 애플리케이션, 회사에서 빌드한 클라우드 기반 애플리케이션 같은 내부 리소스에 액세스 할 때 유용한 기능을 한다
- AAD는 조건부 액세스 및 Identity Protection 같은 기능을 통해 사용자 ID와 애플리케이션을 안전하게 유지하도록 도와준다
- AAD는 조직을 나타내는 테넌트에 사용자를 저장한다
- 개발자를 위한 그룹과 애플리케이션 테스터를 위한 또 다른 그룹을 만드는 것처럼 각 테넌트는 여러 사용자로 구성된 여러 그룹을 포함할 수 있으며, 각 그룹마다 다른 액세스 수준을 갖는다

<AAD 사용자>

- Azure AD는 다양한 유형의 사용자의 요구를 충족한다
- 관리자는 Azure AD를 사용하여 회사 요구 사항에 따라 애플리케이션 및 리소스에 대한 액세스 권한을 부여할 사용자를 결정할 수도 있고, 로그인 시 다단계 인증을 적용하여 애플리케이션 및 서비스에 다른 보호 계층을 추가할 수도 있다
- 개발자는 Azure AD를 사용하여 사용자가 기존 자격증명을 사용하여 애플리케이션에 액세스하도록 할 수 있고, 특정 API를 통해 조직의 사용자 데이터에 액세스하여 맞춤형 최종 사용자 환경을 만들 수도 있다

<AAD 보안점수>

- 관리자는 ID 보안 점수를 통해 AAD 테넌트(전체조직)의 보안유지 방법을 알고 있어야 한다
- 사용자 MS에서 테넌트 보안을 위해 제안하는 권장사항 및 모범사례에 얼마나 일치하지는를 나타내는 1~223 사이의 점수가 지정된다
- 이는 보안이 얼마나 효과적이었는지 표시하며 기능을 개선하는데 도움이 된다



<Azure AD vs Active Directory>

| 서비스 | 인증 | 구조체 | 사용 대상 |
|------------------------|-------------------------------|---------------------|---|
| Active Directory | Kerberos, NTLM | 포리스트, 도메인, 조직 구성 단위 | 온-프레미스 프린터, 애플리케이션, 파일 서비스 등에 대한 인증 및 권한 부여 |
| Azure Active Directory | SAML, OAuth, WS-Federation 포함 | 테넌트 | 인터넷 기반 서비스 및 애플리케이션(예: Microsoft 365, Azure 서비스 및 타사 SaaS 애플리케이션) |



- Azure AD는 AD를 대체하지 않아 어느 서비스를 사용할지는 조직의 요구사항에 따라 달라지며, 두 서비스를 함께 사용할 수도 있다

<Hybrid ID>

- 사용자들이 클라우드와 온프레미스 모두에서 애플리케이션에 액세스하기를 원할 때, AAD와 AD에서 함께 사용할 수 있는 ID 솔루션
- 인증을 위한 사용자가 해당 ID를 가지고 있으면 위치와 관계없이 애플리케이션 및 리소스에 액세스 할 수 있다

<Azure AD 라이선스>

- 라이선스에 유형에 따라 Azure AD의 다양한 기능을 사용할 수 있다
- Azure Active Directory Free. 사용자 및 그룹을 관리하고, 온-프레미스 Active Directory 등기화 및 Azure AD 사용자에 대한 셀프 서비스 암호 재설정과 관련된 기본 보고서를 얻을 수 있습니다. 또한 Microsoft 365, Azure 서비스 및 많은 타사 SaaS 애플리케이션에서 Single Sign-On을 사용할 수도 있습니다.
- Azure Active Directory Premium P1. 이 라이선스를 통해 Free 계층의 모든 기능을 사용할 수 있으며, 사용자가 온-프레미스 및 클라우드 기반 서비스와 리소스에 액세스할 수도 있습니다. 지정된 조건에 따라 사용자를 자동으로 추가하고 제거하는 동적 그룹 또는 셀프 서비스 그룹 관리도 사용할 수 있습니다. 이 계층은 Microsoft Identity Manager 같은 온-프레미스 ID 관리 그룹을 지원합니다. 셀프 서비스 암호 재설정은 온-프레미스를 기준으로 하는 사용자에 대해서도 지원됩니다.
- Azure Active Directory Premium P2. Active Directory ID 보호와 함께 이전 두 계층의 모든 기능을 사용할 수 있습니다. 이 기능을 사용하면 애플리케이션은 ID 위험으로부터 보호하기 위해 위험 기반 조건부 액세스를 구성할 수 있습니다. 또한 Privileged Identity Management를 사용하여 관리자를 모니터링하고 관리자에 세부적인 제한을 적용할 수 있습니다.
- 특정 기능에 대한 종량제 라이선스. Azure AD B2C와 같은 특정 Azure AD 기능은 종량제로 액세스됩니다. Azure AD B2C를 사용하면 소비자 사용자 및 이들이 사용하는 애플리케이션에 대한 ID 및 액세스를 관리할 수 있습니다.

<Azure AD 용어>

1. **ID**
 - 식별하고 인증해야 하는 대상으로, 일반적으로 사용자 이름 및 암호 자격증명을 가진 사용자이지만, 애플리케이션 또는 서비스에도 적용될 수 있다
2. **계정**
 - ID 및 연결된 데이터를 의미, 계정은 ID 없이 존재 할 수 없다
3. **AAD 계정**
 - AAD 또는 MS 365와 같은 서비스에서 만든 ID, 이는 AAD에 저장된다
4. **Azure AD 테넌트**
 - Azure AD의 인스턴스를 의미하며, Azure 또는 다른 서비스에 처음 등록할 때 자동으로 생성된다
 - 조직을 나타내는 테넌트는 사용자, 사용자 그룹, 애플리케이션을 보유한다
5. **다중 테넌트**
 - 공유 환경에서 동일한 애플리케이션 및 서비스에 대한 다중 테넌트 액세스, 여러 조직을 나타낸다
6. **Azure AD 디렉터리**
 - Azure를 구독할 때 자동으로 생성되는 Azure 리소스, 여러 디렉터리를 생성 할 수 있다
 - 이러한 각 디렉터리는 테넌트를 나타낸다
7. **사용자 지정 도메인**
 - Azure AD 디렉터리에 맞게 사용자 지정하는 도메인, 디렉터리를 생성할 때, 'gksehdwns117naver.onmicrosoft.com'과 같이 기본 도메인이 자동으로 할당된다
 - 도메인 이름은 생성 시 사용자 지정 이름으로 설정할 수 있다
8. **소유자 역할**
 - Azure 모든 리소스를 관리하는데 사용하는 역할로, 사용자가 리소스에 대해 필요로 하는 액세스 수준이 필요하다

9. 전역관리자

- Azure AD의 모든 관리 기능에 액세스 할 수 있는 역할, 테넌트를 만들때 해당 테넌트에 해당 역할이 자동으로 적용된다

- 해당 역할이 있는 테넌트는 사용자 권한과 모든 사용자 및 관리자에 대해 암호를 다시 설정 할 수 있다

10. Azure AD PIM(Privileged Identity Management)

- 역할 할당, 셀프 서비스 및 Just-in-Time 역할 활성화를 감독하고 Azure AD 및 Azure 리소스 액세스를 검토할 수 있는 추가 유료 제품이다

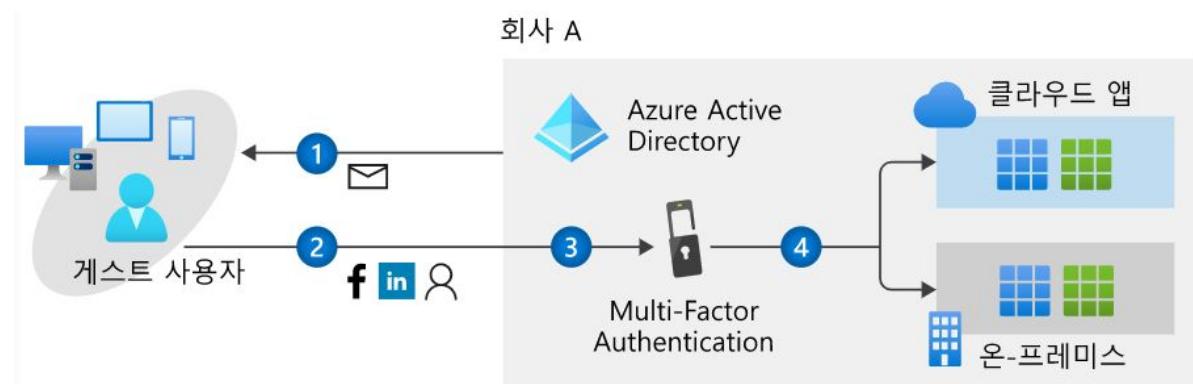
<기본 사용자 권한>

Azure AD는 테넌트의 모든 사용자에게 기본 권한 집합을 제공합니다. 권한은 사용자가 수행할 수 있는 작업과 수행할 수 없는 작업을 지정합니다. 기본적으로 부여되는 권한 세트는 사용자가 테넌트의 멤버(예: 내부 직원)인지 아니면 외부 조직의 멤버인지에 따라 달라집니다. 후자는 게스트로 간주됩니다. 게스트의 예로는 여러분을 위해 일하는 공급업체가 있지만 조직의 공식 직원은 게스트가 아닙니다. 게스트 사용자는 Azure Active Directory B2B라고 하는 Azure AD 기능을 통해 테넌트에 초대됩니다.

멤버 사용자는 게스트 사용자는 불가능한 여러 작업을 수행할 수 있습니다. 예를 들어 멤버 사용자는 전화 번호 및 프로필 사진 등 본인의 프로필 세부 정보를 관리합니다. 게스트 사용자에게는 일반적으로 더 많은 제한이 있습니다. 예를 들어 게스트 사용자는 표시 사진을 볼 수 있지만 변경할 수는 없습니다. 회사에서 정기적으로 작업하는 외부 의뢰 전문가에게는 게스트 사용자 액세스 권한을 부여할 수 있습니다. 이러한 방식으로 일반적인 내부 직원보다는 제한된 권한이지만 작업을 수행할 수 있는 충분한 권한을 갖게 됩니다.

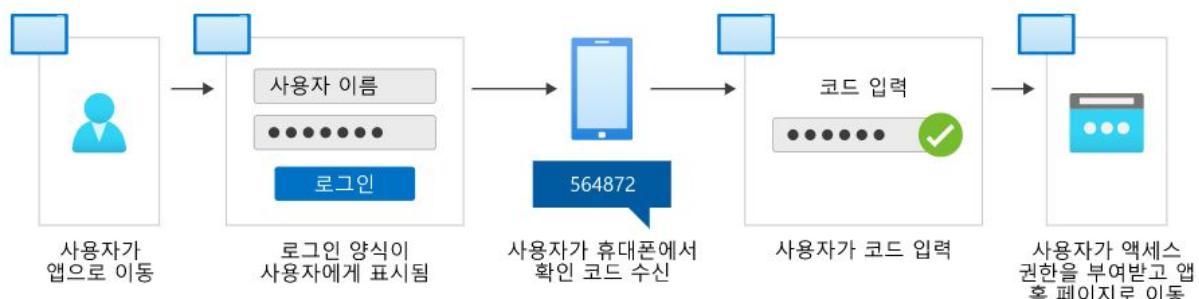
<Azure AD B2B> Business to Business

- 외부 사용자(ex. 외부 파트너..)를 게스트 사용자로 테넌트에 초대하는 기능
- 해당 기능은 AD의 모든 라이선스 계층에서 사용 할 수 있다



<Azure AD B2C> Business to Customer

- 고객의 ID와 액세스 관리를 하는 기능, 모든 계정은 리소스 및 서비스에 대한 보호된 액세스 권한이 있어야 한다
- 사용자 계정에 대한 무차별 암호대입 공격 및 서비스 거부 공격과 같은 위협을 모니터링하는데 도움이 된다
- 해당 기능을 사용하려면 애플리케이션을 등록하고, 애플리케이션에 액세스하는 사용자 경험을 설정하도록 사용자 흐름을 구성한다
- 해당 기능은 종량제로 사용할 수 있다



<Azure AD Domain Service>

- 도메인 컨트롤러가 없어도 도메인에 가상머신을 추가할 수 있는 기능
- 내부 직원 사용자는 회사 Azure AD 자격증명을 사용하여 가상머신에 액세스 할 수 있다
- 해당 서비스를 사용하여 온프레미스 애플리케이션을 Azure로 마이그레이션하는 복잡성을 줄일 수 있다
- 해당 서비스를 사용하여 조직에서는 온프레미스 및 클라우드 둘다에서 애플리케이션을 실행하는 인프라를 처리 할 수 있다
- Azure AD Connect Sync는 Azure AD에서 온프레미스 AD와 조직의 테넌트간에 ID정보를 동기화한다
- 회사는 Azure AD 테넌트에서 Azure AD DS를 사용하도록 설정하고, Azure의 애플리케이션 및 서버에서 도메인 가입, Kerberos 인증 등의 기능을 사용할 수 있다
- 해당 기능은 관리하는 도메인의 총 개체 수를 기준으로 종량제로 사용할 수 있다

<Azure AD ID 보호>

- 사용자에 대한 ID 위협을 자동으로 감지, 조사 및 수정 할 수 있는 기능이다
- ID 보호를 사용하여 위협에 대해 수집된 모든 정보를 내보낼 수도 있고, 추가 분석을 수행할 수 있도록 해당 정보를 타사 도구 및 솔루션으로 내보낼 수도 있다

- ID 보호는 위험정책을 사용하여 자동으로 위협을 감지하고 대응하며, 특정 유형의 위험에 대응할 방법을 설정하는 위험 정책을 구성하고, 이러한 방식으로 정책을 사용하여 시간을 절약하고 안심하고 작업할 수 있다
- 자동화된 위험 검색 및 설정을 사용하여 관리자는 먼저 위험정책을 구성하고, ID 위험여부를 모니터링, 위험이 감지되면 정책은 이를 해결하기 위한 조치를 적용한다
ex. 위험정책은 사용자위험을 감지하고 사용자에게 암호를 다시 설정하도록 요청



Azure Active Directory를 사용한 SSO

또한 SSO에 Azure AD를 활용하면 여러 데이터 원본을 인텔리전트 보안 그래프로 결합할 수 있습니다. 이 보안 그래프를 통해 온-프레미스 AD에서 동기화된 계정을 포함하여 Azure AD의 모든 계정에 위협 분석 및 실시간 ID 보호 기능을 제공할 수 있습니다. 중앙 집중식 ID 공급자를 사용하면 ID 인프라의 보안 제어, 보고, 경고 및 관리를 중앙 집중화할 수 있습니다.

Contoso Shipping는 기존 Active Directory 인스턴스를 Azure AD와 통합하여 조직 전체에서 액세스를 일관적으로 제어할 수 있습니다. 이렇게 하면 다시 인증하지 않고 이메일 및 Microsoft 365 문서에 간단하게 로그인할 수 있습니다.

Azure의 암호화

<원격 스토리지 암호화>

- Azure 스토리지 플랫폼은 자동으로 데이터를 암호화 한 후, Azure Managed Disks, Azure Blob/Queue 스토리지, Azure files에 보관하고 데이터를 암호 해독한 후 검색한다

<가상 머신 디스크 암호화>

- Windows 및 Linux의 IaaS 가상 머신 디스크를 암호화 할 수 있는 기능
- Windows의 BitLocker 기능과 Linux의 DM-Crypt 기능을 활용하여 OS 및 데이터 디스크를 위한 볼륨 암호화를 제공한다
- 고객이 디스크 암호화 키 및 기밀을 관리, 관리 서비스 ID를 사용하여 Key Vault에 액세스 할 수 있도록 Azure Key Vault와 통합된다

<데이터베이스 암호화>

- TDE(투명한 데이터 암호화)는 악의적인 활동의 위협으로부터 Azure SQL DB, Azure Data Warehouse를 보호하는 데 도움을 준다
- 애플리케이션에 대한 변경 없이 미사용 데이터베이스, 연결된 백업 및 트랜잭션 로그 파일의 실시간 암호화 및 암호 해독을 수행한다
- 새로 배포된 Azure SQL DB 인스턴스에는 기본적으로 TDE가 사용된다 |
- TDE는 데이터베이스 암호화 키라는 대칭키를 사용하여 전체 데이터베이스의 스토리지를 암호화한다
- Azure Key Vault에 저장된 키를 통해 BYOK(Bring Your Own Key)도 지원된다

<Azure Key Vault>

- 애플리케이션의 기밀을 하나의 중앙 위치에 보관하고 보안 액세스, 권한 제어 및 액세스 로깅 기능을 제공하므로 애플리케이션의 비밀을 제어하는 중앙 집중형 클라우드 서비스
- 애플리케이션 비밀 스토리지를 중앙 집중화하면 배포를 제어하고 기밀이 우발적으로 누출될 가능성을 줄일 수 있다
- Key Vault를 사용하면 회사 기밀에 대한 액세스를 모니터링하고 제어할 수 있다
- 공용 CA 인증 기관의 인증서를 간단하게 등록하고 간편 할 수 있다
- 여러 Azure 서비스(스토리지 계정, 컨테이너 레지스트리, 이벤트 허브 ...)를 Key Vault와 통합 할 수 있다
- 키, 토큰, 인증서, API 키를 안전하게 저장하고 엄격하게 제어하는 기능
- **비밀 관리**: Key Vault를 사용하여 토큰, 암호, 인증서, API(애플리케이션 프로그래밍 인터페이스) 키 및 기타 비밀에 대한 액세스를 안전하게 저장하고 엄격하게 제어할 수 있습니다.
- **키 관리**: Key Vault를 키 관리 솔루션으로 사용할 수도 있습니다. Key Vault를 사용하면 데이터를 암호화하는 데 사용되는 암호화 키를 쉽게 만들고 제어할 수 있습니다.
- **인증서 관리**: Key Vault를 사용하면 Azure 및 내부적으로 연결된 리소스에 사용할 퍼블릭 및 프라이빗 SSL/TLS(Secure Sockets Layer/전송 계층 보안) 인증서를 보다 쉽게 프로비전, 관리 및 배포할 수 있습니다.
- **HSM(하드웨어 보안 모듈)**으로 백업되는 **비밀 저장**: 비밀과 키는 소프트웨어 또는 FIPS 140-2 Level 2 검증을 받은 HSM을 통해 보호할 수 있습니다.

Azure 네트워크 보호

- 네트워크 경계에서 보호를 시작하는 경우 인터넷 공격을 제한하고 제거하는 것에 집중한다
- 인터넷에 연결되는 리소스를 평가하고 필요한 경우에만 인바운드 및 아웃바운드 통신을 허용하는 것이 좋다
- 모든 종류의 인바운드 네트워크 트래픽을 허용하는 리소스를 식별하고, 리소스를 반드시 필요한 포트/프로토콜로 제한해야 한다

- 네트워크 보안그룹이 연결되지 않은 인터넷 연결 리소스와 방화벽의 보호를 받지 않는 리소스를 식별하기 위하여 Azure Security Center에서 정보를 찾아보는 것이 좋다

<방화벽>

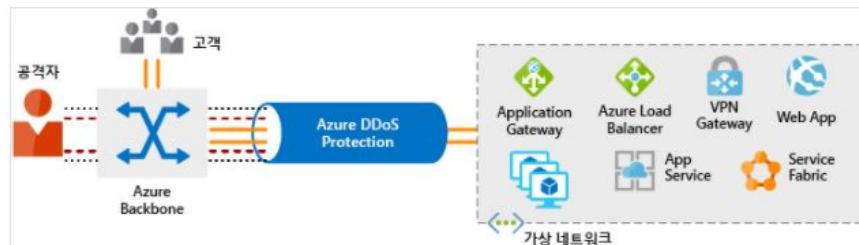
- 각 요청의 원래 IP 주소에 따라 서버 액세스 권한을 부여하는 서비스
 - IP 주소 범위를 지정하는 방화벽 규칙을 만들고, 이러한 권한이 부여된 IP 주소의 클라이언트만 서버에 액세스 할 수 있다
 - 일반적으로 방화벽 규칙에는 특정 네트워크 프로토콜 및 포트 정보도 포함된다
- Azure Firewall**
 - Azure Virtual Network 리소스를 보호하는 관리되는 클라우드 기반 네트워크 보안 서비스
 - 고가용성 및 무제한 클라우드 확장성이 내장되어 있는 서비스 형태의 완전한 상태 저장 방화벽
 - 비(?) HTTPS 프로토콜(SSH,RDP,FTP..)에 대한 인바운드 보호를 제공한다
 - 모든 포트 및 프로토콜에 아웃바운드 네트워크 수준 보호를 제공하고 아웃바운드 HTTPS에 애플리케이션 수준 보호를 제공한다
 - Azure Application Gateway**
 - 웹 사이트의 널리 알려진 취약성으로부터 보호하는 WAF(웹 애플리케이션 방화벽)이 포함된 부하 분산 장치이다
 - HTTP 트래픽을 보호하도록 설계되었다
 - NVA(네트워크 가상 어플라이언스)**
 - HTTP가 아닌 서비스 또는 고급 구성에 적합한 옵션이며, 하드웨어 방화벽 어플라이언스와 비슷하다

<DDoS 방지>

- 인터넷에 공개된 모든 리소스는 서비스 거부 공격(DDoS)을 받을 위험이 항상 존재한다

1. Azure DDoS Protection

- MS의 대규모 글로벌 네트워크를 활용하여 모든 Azure 지역에 DDoS 완화능력을 제공한다
- Azure 네트워크 트래픽이 서비스의 가용성에 영향을 주기 전에 해당 트래픽을 모니터링하여 Azure 애플리케이션을 보호한다
- 공격이 감지되면 몇 분 이내에 Azure Monitor 메트릭을 사용한 알림은 받는다
- 네트워크에 과도한 부하를 걸려고 하는 공격자의 시도를 식별하고 더 이상의 트래픽이 Azure 서비스에 도달하는 것을 차단한다



- 기본 - 기본 서비스 계층은 Azure 플랫폼의 일부로 자동으로 사용하도록 설정됩니다. 일반적인 네트워크 수준 공격에 대한 항시 트래픽 모니터링과 실시간 완화는 Microsoft의 온라인 서비스에서 사용하는 것과 동일한 방어를 제공합니다. Azure의 글로벌 네트워크는 Azure 지역에 대한 공격 트래픽을 분산하고 완화하는 데 사용됩니다.
- 표준 - 표준 서비스 계층은 Microsoft Azure Virtual Network 리소스에 맞게 특별히 조정된 추가적인 완화 기능을 제공합니다. DDoS Protection 표준은 간단히 사용하도록 설정할 수 있고 애플리케이션을 변경할 필요가 없습니다. 보호 정책은 전용 트래픽 모니터링 및 기계 학습 알고리즘을 통해 조정됩니다. 정책은 Azure Load Balancer, Application Gateway 등의 가상 네트워크에 배포된 리소스와 연결된 공용 IP 주소에 적용됩니다. DDoS 표준 보호는 다음 유형의 공격을 완화할 수 있습니다.
 - 대규모 공격. 이 공격의 목표는 정상적으로 보이는 대량의 트래픽으로 네트워크 계층을 마비시키는 것입니다.
 - 프로토콜 공격. 이 공격은 계층 3 및 계층 4 프로토콜 스택의 취약점을 악용하여 대상을 액세스 불능 상태로 만듭니다.
 - 리소스(애플리케이션) 계층 공격. 이 공격은 대상 웹 애플리케이션 패킷을 공격하여 호스트 간 데이터 전송을 방해합니다.

<가상 네트워크 내부의 트래픽 제어>

- 가상 네트워크 내에서는 꼭 필요한 곳에서만 리소스 간 통신이 이루어지도록 제한해야 한다
 - 가상 머신간의 통신에는 NSG(네트워크 보안 그룹)를 통해 불필요한 통신을 제한하는 것이 중요하다
- NSG(네트워크 보안 그룹)**
 - 네트워크 보안 그룹을 사용하면 Azure 가상 네트워크의 Azure 리소스와 주고 받는 네트워크 트래픽을 필터링 할 수 있다
 - 각 NSG에는 원본 및 대상 IP 주소, 포트 및 프로토콜을 기준으로 리소스와 주고 받는 트래픽을 필터링 할 수 있는 여러 개의 인바운드 및 아웃바운드 보안 규칙이 포함 될 수 있다
 - 네트워크 인터페이스 및 서브넷과 허용되거나 거부되는 통신의 목록을 제공하며 완전히 사용자 지정 할 수 있다
 - VPN(가상 사설망)**
 - 네트워크간에 보안 통신 채널을 설정하는 일반적인 방법이다
 - Azure 가상 네트워크와 온프레미스 VPN 디바이스 연결하는 것이 일반적인 방법이다
 - Azure ExpressRoute**
 - ExpressRoute를 사용하면 연결 공급자가 지원하는 프라이빗 연결을 통해 온프레미스 네트워크를 클라우드로 확장 할 수 있다
 - 해당 연결은 공용 인터넷 대신 프라이빗 회로를 통해 이 트래픽을 전송하여 온프레미스 통신의 보안을 개선한다
 - 공용 인터넷을 통해 이 서비스에 액세스하도록 허용할 필요가 없으며, 어플라이언스를 통해 이트래픽을 전송하여 트래픽을 추가로 검사할 수 있다

공유 문서보호

<Azure Information Protection(AIP)>

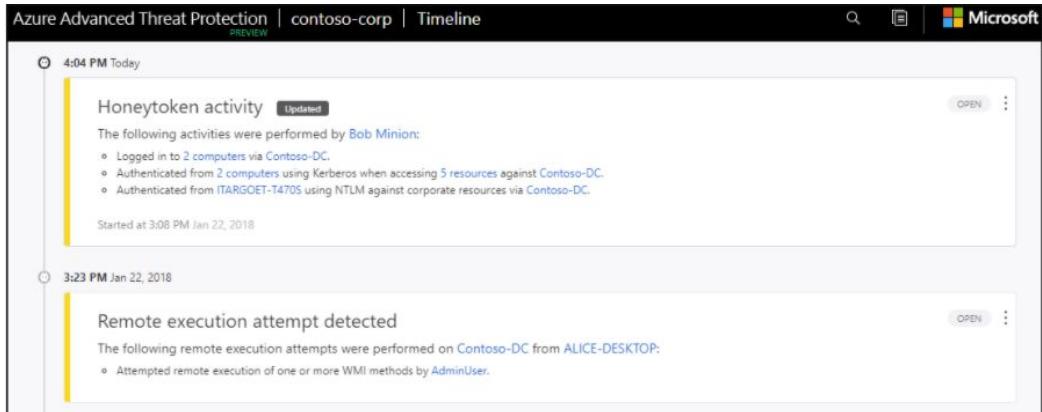
- 조직에서 레이블을 적용하여 문서와 메일을 분류하고 필요에 따라 보호할 수 있게 도와주는 클라우드 기반 솔루션
- 규칙 및 조건에 따라 자동 또는 레이블을 적용하고, 이 단계를 결합하여 사용자에게 권장 레이블을 안내 할 수도 있다
- 문서 및 이메일, 메세지, 신용카드 정보등 중요한 데이터를 보호/암호 할 때 사용한다

Azure Advanced Threat Protection (Azure ATP)

- 고객의 조직을 노리는 고급 위협, 손상된 ID 및 악의적인 내부자 작업을 식별, 탐지, 조사하도록 도와주는 클라우드 기반 보안 솔루션
- Azure ATP는 알려진 악의적인 공격과 기법, 보안 문제 및 네트워크 위협을 탐지 할 수 있다

1. Azure ATP 포털 (<https://portal.atp.azure.com>)

- Azure ATP는 자체 포털을 갖고 있으며, 이포털을 통해 의심스러운 활동을 모니터링하고 적절하게 대응 할 수 있다
- 자체 포털을 통해 ATP 인스턴스를 만들고, 센서에서 받은 데이터를 볼 수 있고, 네트워크 환경의 위협을 모니터링, 관리 및 조사할 수도 있다



The screenshot shows the Azure Advanced Threat Protection (Azure ATP) portal interface. At the top, it displays 'Azure Advanced Threat Protection | contoso-corp | Timeline'. Below the timeline, there are two main alert cards:

- Honeytoken activity** (Updated): Occurred at 4:04 PM Today. It details activity performed by Bob Minion:
 - Logged in to 2 computers via Contoso-DC.
 - Authenticated from 2 computers using Kerberos when accessing 5 resources against Contoso-DC.
 - Authenticated from ITARGOET-T4705 using NTLM against corporate resources via Contoso-DC.It also notes it started at 3:08 PM Jan 22, 2018.
- Remote execution attempt detected**: Occurred at 3:23 PM Jan 22, 2018. It details attempts from ALICE-DESKTOP:
 - Attempted remote execution of one or more WMI methods by AdminUser.

2. Azure ATP 센서

- 도메인 컨트롤러에 직접 설치되는 기능이다. 해당 센서는 전용 서버 없이 또는 포트 미러링을 구성하지 않고도 도메인 컨트롤러 트래픽을 모니터링한다

3. Azure ATP 클라우드 서비스

- Azure 클라우드 인프라에서 실행되며 현재 미국, 유럽 및 아시아에 배포된다

Azure 가격 책정 서비스 수준 계약 수명 주기 설명

Azure Policy

- 일관된 클라우드 인프라를 계획하려면 먼저 정책을 설정해야 한다
- 만든 리소스에 대한 규칙이 정책을 통해 적용되므로 인프라는 고객에게 제공하는 회사 표준, 비용 요구 사항 및 SLA를 준수하게 된다
- Azure Policy는 정책을 만들고, 할당하고, 관리하는데 사용하는 서비스이다
- 해당 정책은 리소스에 대해 다양한 규칙과 효과를 적용하여 리소스를 회사 표준 및 서비스 수준 계약을 준수하는 상태로 유지한다
- Azure Policy는 할당된 정책의 비준수에 대해 리소스를 평가하여 이 요구를 충족한다

조직의 모든 사용자가 VM(가상 머신)을 만들 수 있도록 허용한다고 가정합니다. 비용을 제어하려고 하므로 Azure 테넌트의 관리자는 4개를 초과하는 CPU가 있는 VM을 만들 수 없도록 하는 정책을 정의합니다. 정책이 구현되면 Azure Policy에서 모든 사용자가 허용되는 SKU(Stock Keeping Unit) 목록에 없는 새 VM을 만들지 못하도록 합니다. 또한 기존 VM을 업데이트하려고 하면 해당 VM이 정책에 따라 검사됩니다. 마지막으로 Azure Policy는 조직의 기존 VM을 모두 감사하여 정책이 적용되도록 합니다. 규정을 준수하지 않는 리소스를 감사하거나, 리소스 속성을 변경하거나, 리소스를 만들지 않도록 중지할 수 있습니다. 애플리케이션의 사전 배포 및 사후 배포에 영향을 주는 연속 통합 및 업데이트 파이프라인 정책을 적용하여 Azure Policy를 Azure DevOps와 통합할 수도 있습니다.

<Azure Policy vs RBAC>

- Azure Policy는 RBAC(역할 기반 액세스 제어)와 같이 특정 리소스 종류에 대한 액세스를 제한하는 방법으로 보일 수 있지만, 이와 다른 문제를 해결한다
- RBAC는 다른 범위에 있는 사용자 작업에 중점을 두고, 리소스 그룹에 대한 기여자 역할에 추가되어 해당 리소스 그룹에 있는 모든 항목을 변경할 수 있다
- 반면 Azure Policy는 배포 시 리소스 속성과 기존 리소스에 중점을 두어 리소스의 유형 또는 위치와 같은 속성을 제어한다
- RBAC와 달리 Azure Policy는 기본적으로 허용 및 명시적 거부 시스템이다

<Azure 정책 만들기 & 정책정의>

- Azure Policy를 만들고 구현하는 프로세스는 '정책정의'를 만드는 것으로 시작된다
- 정책정의란? 평가할 항목과 수행할 작업을 나타낸다 예를 들어, 모든 공용 웹사이트가 HTTPS로 보호되는지 확인하거나, 특정 스토리지 유형을 만들지 않도록 하거나, 특정 버전의 SQL Server를 사용하도록 강제로 적용 할 수 있다
- 적용 할 수 있는 가장 일반적인 정책 정의는 아래 그림과 같다

| 정책 정의 | 설명 |
|---|---|
| 허용되는 스토리지 계정 SKU | 이 정책 정의에는 배포 중인 스토리지 계정이 SKU 크기 세트 내에 있는지 여부를 결정하는 조건/규칙 세트가 있습니다. 해당 효과는 정의된 SKU 크기 세트를 준수하지 않는 모든 스토리지 계정을 거부하는 것입니다. |
| 허용되는 리소스 종류 | 이 정책 정의에는 조직에서 배포할 수 있는 리소스 종류를 지정하는 조건/규칙 세트가 있습니다. 해당 효과는 정의된 목록에 속하지 않은 모든 리소스를 거부하는 것입니다. |
| 허용되는 위치 | 이 정책을 사용하면 조직에서 리소스를 배포할 때 지정할 수 있는 위치를 제한할 수 있습니다. 해당 효과는 지리적 규정 준수 요구 사항을 적용하는 데 사용됩니다. |
| 허용되는 Virtual Machine SKU | 이 정책을 사용하면 조직에서 배포할 수 있는 VM SKU 세트를 지정할 수 있습니다. |
| 허용되지 않는 리소스 종류 | 리소스 종류 목록이 배포되지 않도록 합니다. |
| <pre>{ "if": { "allOf": [{ "field": "type", "equals": "Microsoft.Compute/virtualMachines" }, { "not": { "field": "Microsoft.Compute/virtualMachines/sku.name", "in": "[parameters('listOfAllowedSKUs')]" } }] }, "then": { "effect": "Deny" } }</pre> | - 정책 정의 자체는 JSON 파일로 표시되며, 포털에서 미리 정의된 정의 중 하나를 사용하거나 사용자 고유의 정의를 만들 수 있다 |

< 특정 가상 머신 SKU만 허용하는 컴퓨팅 정책

<정책 적용>

- 정책을 적용하려면 Azure Portal을 사용하거나, Microsoft.Policy Insights 확장을 추가하여 Azure Powershell과 같은 명령줄 도구를 사용 할 수 있다

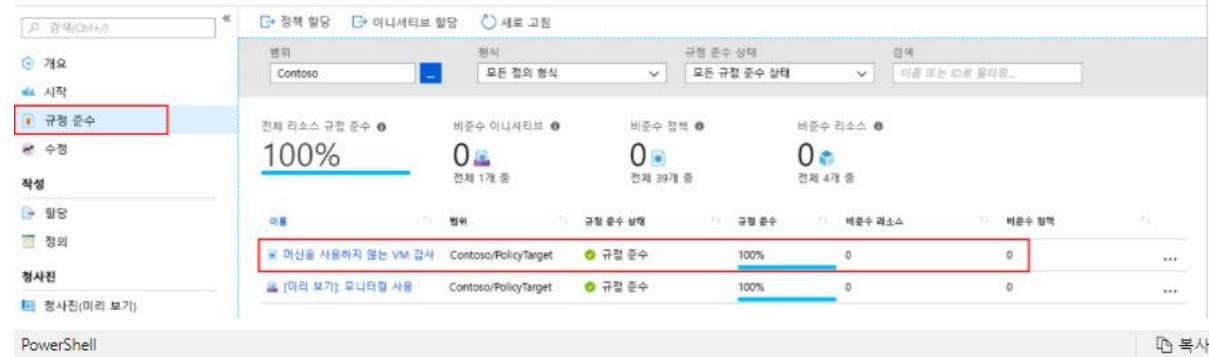
PowerShell

```
# Register the resource provider if it's not already registered
Register-AzResourceProvider -ProviderNamespace 'Microsoft.PolicyInsights'
```

<비규격 리소스 식별>

- 적용된 정책 정의를 사용하여 Azure Portal을 통해 정책할당을 준수하지 않는 리소스를 식별할 수 있다
- 결과는 Azure Portal에서 정책할당의 리소스 규정 준수 탭에 보이는 것과 일치한다
- 또는 명령줄 도구를 사용하여 리소스 그룹에서 정책할당을 준수하지 않는 리소스를 식별 할 수 있다

정책 및 규정 준수



PowerShell

```
Get-AzPolicyState -ResourceGroupName $rg.ResourceGroupName -PolicyAssignmentName 'audit-vm-manageddisks' -Filter 'IsCompliant eq false'

Timestamp : 3/9/19 9:21:29 PM
ResourceId : /subscriptions/{subscriptionId}/resourcegroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/contoso-vm
PolicyAssignmentId : /subscriptions/{subscriptionId}/providers/microsoft.authorization/policyassignments/audit-vm-manageddisks
PolicyDefinitionId : /providers/Microsoft.Authorization/policyDefinitions/06a78e20-9358-41c9-923c-fb736d382a4d
IsCompliant : False
SubscriptionId : {subscriptionId}
ResourceType : /Microsoft.Compute/virtualMachines
ResourceTags : tbd
PolicyAssignmentName : audit-vm-manageddisks
PolicyAssignmentOwner : tbd
PolicyAssignmentScope : /subscriptions/{subscriptionId}
PolicyDefinitionName : 06a78e20-9358-41c9-923c-fb736d382a4d
PolicyDefinitionAction : audit
PolicyDefinitionCategory : Compute
ManagementGroupIds : {managementGroupId}
```

(명령줄 결과창)

<리소스 범위에 정의 할당>

- 정책할당은 특정 범위 내에서 수행되도록 할당된 정책으로, 하나 이상의 정책 정의가 정의되면 이를 할당해야 한다
- 정책할당의 범위는 전체 구독에서 리소스 그룹까지 다양하며, 모든 자식 리소스에 상속된다
- 상속되는 것을 원하지 않으면, 하위 범위에서 해당 리소스 그룹을 제외 시킬 수 있다
ex. 모든 구독에 정책을 적용한 후, 선택한 몇 가지 리소스 그룹을 제외 할 수 있다
- Azure Portal, Powershell, Azure CLI를 통해 이러한 정책 중 하나를 할당 할 수 있다
- 정책정의를 할당할 때는 정의되는 매개변수를 모두 제공해야한다

허용되는 가상 머신 SKU

정책 할당

설명

Standard_A2 시리즈를 제외한 모든 VM을 중지합니다.

매개 변수

* 허용되는 SKU

3개 선택됨

<정책 효과>

- Azure Resource Manager를 통해 리소스를 만들거나 업데이트 하도록 요구하는 요청은 먼저 Azure Policy에서 평가된다
- 리소스에 적용되는 모든 할당 목록을 만든 다음, 리소스를 각 정의와 비교하여 평가한다
- 리소스에서 정책을 위반하는 경우 불필요한 처리를 방지하기 위해 Policy는 적절한 리소스 공급자에 요청을 전달하기 전에 여러 가지 효과를 처리한다

| 정책 효과 | 어떻게 되나요? |
|-------------------------|---|
| Deny | 정책으로 인해 리소스 만들기/업데이트가 실패합니다. |
| Disabled | 정책 규칙이 무시됩니다(사용 안 함). 테스트를 위해 자주 사용됩니다. |
| Append | 만들기 또는 업데이트 중에 요청된 리소스에 추가 매개 변수/필드를 추가합니다. 일반적인 예로, 비용 센터와 같은 리소스에 태그를 추가하거나 스토리지 리소스에 허용되는 IP를 지정합니다. |
| Audit, AuditIfNotExists | 규정을 준수하지 않는 리소스를 평가할 때 활동 로그에 경고 이벤트를 만들지만 요청은 중지되지 않습니다. |
| DeployIfNotExists | 특정 조건이 충족되면 템플릿 배포를 실행합니다. 예를 들어 데이터베이스에서 SQL 암호화를 사용하도록 설정되면 DB를 만든 후에 템플릿을 실행하여 특정 방식으로 설정할 수 있습니다. |

<정책 평가 결과 보기>

- Azure Policy를 사용하면 유효성 검사를 통과하지 못한 경우에도 리소스를 만들 수 있다
- 이러한 경우 Azure Policy 포털 또는 명령줄 도구를 통해 볼 수 있는 감사 이벤트를 트리거 할 수 있다
- 가장 쉬운 검색 방법은 훌륭한 그래픽 개요를 제공하는 포털에 있다
- Azure Policy 섹션은 검색 필드 또는 '모든 서비스'를 통해 찾을 수 있다



<정책 할당 제거>

- 마지막으로, Portal, Powershell 명령 'Remove-AzPolicyAssignment'를 통해 정책 요구 사항을 삭제할 수 있다

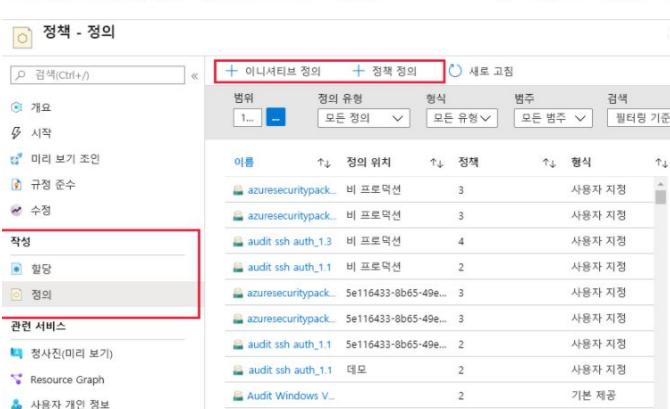
```
PowerShell
```

```
Remove-AzPolicyAssignment -Name 'audit-vm-manageddisks' -Scope '/subscriptions/<subscriptionID>/resourceGroups/<resourceGroupName>'
```

<이니셔티브>

- 이니셔티브는 Azure Policy의 정책과 함께 작동하는 규정 준수 상태를 추적하는데 도움이 되는 정책정의의 세트 또는 그룹이다.
- 단일 정책일 경우에도 시간이 지남에 따라 정책 수가 증가할 것을 대비하여 이니셔티브를 사용하는 것이 좋다
- 이니셔티브가 정의되면 정책과 마찬가지로 할당 될 수 있으며, 모든 관련 정책 정의가 적용된다
- 이니셔티브의 정의는 정책 세트를 단일 항목으로 그룹화하여 정책정의를 관리하고 할당하는 프로세스를 간소화한다

| 정책 정의 | 목적 |
|--|-------------------------------------|
| Security Center에서 암호화되지 않은 SQL Database 모니터링 | 암호화되지 않은 SQL 데이터베이스와 서버를 모니터링합니다. |
| Security Center에서 OS 취약성 모니터링 | 구성된 기준을 충족하지 않는 서버를 모니터링합니다. |
| Security Center에서 누락된 Endpoint Protection 모니터링 | 엔드포인트 보호 애이전트가 설치되지 않은 서버를 모니터링합니다. |

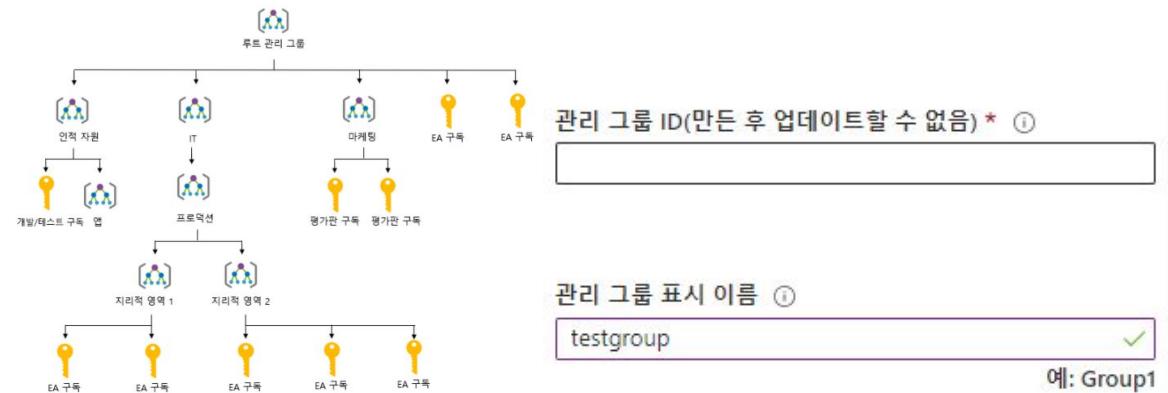


여러 Azure 구독에서 액세스, 정책 및 규정 준수 관리

- 액세스 관리는 Azure 구독 수준에서 수행된다. 조직에서는 회사의 각 사업부를 책임과 요구사항에 따라 특정 방식으로 구성할 수 있다

<관리 그룹을 사용하여 구독 관리>

- Azure 관리그룹은 여러 Azure 구독에서 액세스, 정책 및 규정 준수를 관리하기 위한 컨테이너이다
- 관리그룹을 사용하면 구독 수준보다 높은 수준의 추가 분류 수준을 제공하는 컬렉션에 Azure 리소스를 계층적으로 정렬 할 수 있다
- 관리그룹에 속한 모든 구독은 관리그룹에 적용되는 조건을 자동으로 상속한다
- 관리그룹은 사용하는 구독 유형에 관계 없이 대규모의 엔터프라이즈급 관리를 제공한다
- 관리그룹을 사용하는 또 다른 유형으로는 여러 구독에 대한 사용자 액세스를 제공하는 것이다
- 해당 관리그룹에서 여러 구독을 이동하면 하나의 RBAC 할당을 관리그룹에 만들 수 있다
즉, 관리그룹에 RBAC를 하나만 할당하면 필요한 여러 구독에 액세스 할 수 있다
- 관리그룹에 할당하는 리소스 및 구독은 해당 관리그룹에 적용하는 모든 조건을 자동으로 상속한다
- 관리그룹 생성시 ID는 고유한 식별자로, 수정 할 수 없지만 이름은 Portal에서 언제든지 수정이 가능하다



<각 조직의 루트 관리그룹>

- 첫번째 관리그룹을 생성하면 Azure AD 조직에 루트 관리그룹이 생성된다
- 기본적으로 루트 관리그룹의 표시 이름은 테넌트 루트 그룹이며, ID는 Azure AD ID이다
- 이 그룹을 만들면 Azure AD 조직의 기존 구독이 모두 루트 관리그룹의 자식 항목으로 설정된다
- 따라서 하나의 조직에는 하나의 관리그룹 계층구조만 있고, 조직에 하나의 계층구조가 있으면 관리자가 조직 내의 다른 사용자가 우회할 수 없는 전역 액세스 및 정책을 적용할 수 있다
- 루트에 할당되는 모든 항목은 전체 계층 구조에 적용되며, 여기에는 Azure AD 조직내의 모든 관리그룹, 구독, 리소스 그룹, 리소스가 포함된다

관리 그룹에 대한 중요한 팩트

- 조직의 모든 Azure AD 사용자는 관리 그룹을 만들 수 있습니다. 만든 이에게 소유자 역할 할당이 부여됩니다.
- 하나의 Azure AD 조직은 10,000개의 관리 그룹을 지원할 수 있습니다.
- 하나의 관리 그룹 트리는 루트 수준 또는 구독 수준을 제외하고 최대 6개의 깊이 수준을 지원할 수 있습니다.
- 각 관리 그룹은 여러 자식 항목을 가질 수 있습니다.
- 조직에서 구독을 만들면 루트 관리 그룹에 구독이 자동으로 추가됩니다.

Azure BluePrints

- 클라우드 설계자가 조직의 표준, 패턴 및 요구사항을 구현하고 준수하는 반복 가능한 Azure 리소스 집합을 정의할 수 있는 서비스
- 개발팀은 해당 서비스를 통해 네트워킹과 같은 기본 제공되는 구성요소를 사용하여 조직의 규정을 준수하면서 빌드한 신뢰할 수 있는 새환경을 빠르게 빌드하고 배포하여 개발 및 납품 시간을 단축할 수 있다

| 청사진 만들기 | 범위에 적용 | 할당 추적 |
|--|-------------------|----------------------------|
| 일반 또는 조직 기반 패턴을 기반으로 하여 템플릿, 정책, 역할 할당 및 리소스 그룹과 같은 아티팩트를 재사용 가능한 청사진으로 작성합니다. | 하나 이상의 구독에 청사진 적용 | 청사진이 적용되는 위치를 추적하고 조직에서 공유 |

만들기

적용

추적

<Azure Blueprints vs Resource Manager 템플릿>

- Azure BluePrints 서비스는 리소스 그룹, 정책, 역할 할당, Resource Manager 템플릿 배포 세트 등의 환경설정에 도움이 되도록 설계된 패키지이므로, CI/CD 파이프라인을 사용하는 등의 방식으로 해당 패키지를 직접 작성하고 버전을 지정할 수 있다. 최종적으로 감사 및 추적이 가능한 한번의 작업을 통해 구독에 할당된다. 또한 청사진 정의(배포해야 하는 항목)와 청사진 할당(배포된 항목)간의 관계가 유지되며, 이 연결은 배포에 대한 향상된 추적 및 감사를 지원하며 동일한 청사진에서 관리하는 여러 구독을 한번에 업드레이드할 수도 있다

- Resource Manager 템플릿을 통해서도 Blueprints에서 배포에 포함하려고 하는 모든 항목을 생성 할 수 있지만 기본적으로 제공되지 않는 문서이다. Resource Manager 템플릿은 로컬이나 소스제어에 저장되며, 하나 이상의 리소스 배포에 사용되기는 하지만, 해당 리소스가 배포되고 나면 해당 템플릿에 대한 활성 연결과는 관계가 손실된다
- Resource Manager 템플릿 청사진 중 하나만 선택할 필요가 없으며, 기존 개발 및 유지에 관리해 왔던 Resource Manager 템플릿 라이브러리를 Blueprints에서 재사용 할 수도 있다

<Azure Policy와의 차이점>

- 청사진은 일관성과 규정 준수 상태를 유지하기 위해 다시 사용할 수 있는 Azure Cloud Services/보안/디자인 구현 관련 표준/패턴/요구 사항의 포커스별 집합으로 구성된 패키지 또는 컨테이너이다
- 반면, 정책은 배포종/기준 리소스에 대해 적용되는 리소스 속성 중심의 기본 허용 및 명시적 거부 시스템이다. 정책은 구독 내의 리소스가 요구사항과 표준을 준수하는지를 확인하여 클라우드 거버넌스를 지원한다

Azure 비용

- 고객이 요구사항에 맞는 Azure 제품 및 서비스를 선택하면 Azure의 종량제 모델에 따라 계정으로 요금이 청구된다
- 고객이 Azure 리소스에 프로비저닝하면 Azure에서는 해당 리소스에 대한 하나 이상의 미터 인스턴스를 생성하고, 미터는 리소스 사용량을 추적하고, 대금을 계산하는데 사용되는 사용량 레코드를 생성한다
- 미터 및 가격책정은 제품에 따라 다르며, 종종 리소스의 크기 또는 용량에 따라 가격책정 계층이 달라지기도 한다.
- 매월 청구 주기가 끝나면 사용량 값이 고객의 결제 방법에 청구되고 미터가 다시 설정되며, 언제든지 고객은 Azure Portal 청구 페이지에서 현재 사용량의 요약 정보를 살펴보고 이전 청구 주기에 청구된 청구서를 확인할 수 있다
- Azure 리소스는 언제나 사용량에 따라 리소스 대금이 청구된다
ex. VM 할당을 최소화하면 컴퓨팅에 관한 요금이 부과되지 않지만, 디스크 스토리지 비용이 발생한다

<Azure 청구영역>

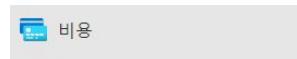
- 대역폭이란 Azure 데이터 센터로 들어오고 나가는 데이터를 의미한다
- 대부분의 인바운드 데이터 전송은 무료이며, 아웃바운드 데이터 전송의 경우 청구 영역에 따라 데이터 전송 가격이 책정된다

| 영역 | 영역 |
|---------|-------------------------------------|
| 영역 1 | 미국, 미국 정부, 유럽, 캐나다, 영국, 프랑스, 스위스 |
| 영역 2 | 동아시아, 동남 아시아, 일본, 오스트레일리아, 인도, 대한민국 |
| 영역 3 | 브라질, 남아프리카 공화국, UAE |
| 독일 영역 1 | 독일 |

- 대부분의 영역에서 매월 처음 아웃바운드 5GB는 무료이고, 이후 초과하면 GB당 고정가격으로 대금이 청구된다

<Azure Advisor 비용 권장사항>

- Azure Advisor는 Azure에 내장된 체험 서비스로, 고비용, 보안, 성능, 뛰어난 운영, 비용에 대한 권장사항을 제공한다
- 배포된 서비스를 분석하여 각 영역에서 환경을 개선할 방법을 탐색한다
- 다음은 비용에 대한 권장 사항의 일부분을 보여준다 ↓



비용 권장 사항을 모두 따르고 있습니다.
[비용 권장 사항 목록 보기](#)

1. 프로비저닝되지 않은 Azure ExpressRoute 회로를 제거하여 비용을 절감합니다. 이 권장 사항은 공급자 상태가 1개월 넘게 '프로비저닝되지 않음'인 ExpressRoute 회로를 식별합니다. Advisor는 연결 공급자로 회로를 프로비저닝하지 않으려는 경우 회로를 삭제할 것을 권장합니다.
2. 예약 인스턴스를 구입하여 종량제 대비 비용을 절감합니다. Advisor는 지난 30일 동안의 가상 머신 사용량을 검토하여 예약 인스턴스 구매 시 앞으로 비용을 절감할 수 있는지 확인합니다. Advisor는 잠재적으로 절감액이 가장 큰 지역과 크기를 보여 주고, 예약 인스턴스 구매로 얻을 수 있는 예상 절감액을 보여 줍니다.
3. 사용률이 낮은 가상 머신을 적합한 크기로 지정하거나 종료합니다. 이 분석은 14일 동안 가상 머신 사용량을 모니터링하여 사용률이 낮은 가상 머신을 식별합니다. 4일 이상 평균 CPU 사용률이 5% 이하이고 네트워크 사용량이 7MB 이하인 가상 머신은 사용률이 낮은 가상 머신으로 간주됩니다. 평균 CPU 활용률 임계값은 최대 20%까지 조정 가능합니다. 이러한 가상 머신을 식별하면 더 작은 인스턴스 유형으로 크기를 조정하도록 결정하여 비용을 절감할 수 있습니다.

<Azure Cost Management>

- 클라우드 비용이 발생하는 부분을 보다 확실하게 파악하기 위해 사용할 수 있는 무료 기본 제공 Azure 도구이다
- 비용을 지출하는 서비스와 설정된 예산 대비 지출을 추적하는 방법에 대한 기록 분석 결과를 볼 수 있고, 예산을 설정하고, 보고서를 예약하고, 비용 영역을 분석할 수 있다

Azure 비용 절감

<Azure 크레딧 사용>

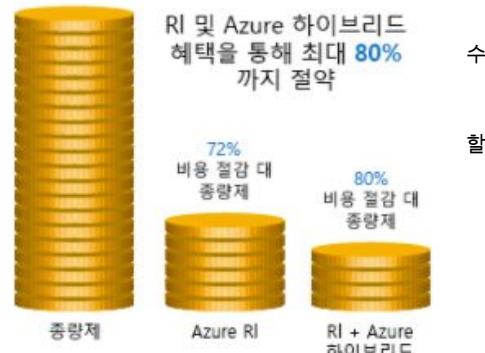
- Visual Studio 구독자는 Azure에서 새 솔루션을 실험, 개발, 테스트 할 수 있는 월간 크레딧 혜택을 활성화 할 수 있다
- Azure 크레딧을 사용하여 App Service, Windows 10 VM, Azure SQL 데이터베이스, Containers, Cognitive Services, Functions, Data Lake 등의 새 서비스를 비용없이 사용할 수 있다
- 해당 혜택을 활성화한 고객은 계정 아래에 별도의 Azure 구독을 소유하게 되고, 활성 Visual Studio 구독자로 남아있는 동안에 매월 갱신되는 월간 크레딧 잔액이 이 구독에 제공된다
 - 월 \$50로 Visual Studio Professional 사용
 - 월 \$150로 Visual Studio Enterprise 사용

<지출 한도 사용>

- 기본적으로 월간 크레딧이 연결된 Azure 구독(평가판 계정 포함)에는 크레딧이 모두 소진되면 더 이상 대금이 청구되지 않도록 방지하는 지출한도가 포함되어 있다
- 지출한도는 구독, 서비스 또는 리소스 그룹 한도 및 할당량과는 다르다
- 지출한도를 활성화하면 월별크레딧이 모두 소진시, 배포한 서비스가 사용하지 않도록 설정되고 해제된다
- 구독의 지출한도에 도달하면 이메일 알림이 제공되며, Azure Portal에는 크레딧 사용량에 대한 알림도 존재한다
- 지출한도 기능은 월별 Azure 크레딧 할당을 포함하는 구독에서만 사용할 수 있으며, 지불 전용 구독에서는 사용할 수 없다

<예약 인스턴스 사용>

- 가상머신 워크로드가 정적이고 예측 가능한 경우, 예약 인스턴스는 비용을 종량제 비용 대비 최대 70~80%까지 절감할 수 있는 매우 유용한 방법이다
- 예약 인스턴스의 약정 기간은 1년 또는 3년이며, 전체 약정 기간의 요금을 전액 결제하거나 매월 약정 금액이 청구되도록 수 있다
- 예약은 Azure Portal에서 구매할 수 있으며, 컴퓨팅 할인에 해당하므로 Windows 및 Linux VM에 모두 사용할 수 있다



<저렴한 위치 및 Azure 지역 선택>

- Azure 제품, 서비스 및 리소스 비용은 위치와 Azure 지역에 따라 달라질 수 있으며, 되도록이면 저렴한 곳을 사용해야 한다

일부 리소스는 나가는 네트워크 대역폭(송신) 사용량을 측정하여 대금이 청구됩니다. 지역 간 송신 트래픽을 줄이려면 동일한 Azure 지역에서 측정되는 대역폭인 연결된 리소스를 프로비전해야 합니다.

<사용률이 낮은 가상머신을 적합한 크기로 지정>

- 과도한 크기의 가상머신은 Azure에서 흔히 볼 수 있는 불필요한 지출 항목임과 동시에 쉽게 해결이 가능하다
- Azure Portal, Azure Powershell, Azure CLI를 통해 VM의 크기를 변경 할 수 있다
- VM의 크기를 조정하려면 VM을 중지하고 크기를 조정한 후 다시 시작하는 것을 권장한다

<업무 외 시간에는 가상머신 할당 취소>

- 특정기간에만 사용되는 가상머신 워크로드를 매일 항상 실행하는 경우는 비용이 낭비되어, 사용하지 않을 때는 종료했다가 일정에 따라 다시 시작하면 VM이 할당 취소된 동안 컴퓨팅 비용을 절감 할 수 있다
- 가상 머신에서 자동종료 기능을 사용하여 예약할 수도 있다

<사용하지 않는 가상머신 삭제>

- 정기적으로 환경을 검토하여 사용하지 않는 VM은 삭제하면 인프라 비용이 절약될 뿐만 아니라 라이선싱 및 운영비용도 잠재적으로 절약되므로 다양한 혜택을 얻을 수 있다

<PaaS 또는 SaaS 서비스로 마이그레이션>

- PaaS 서비스를 사용하면 일반적으로 리소스와 운영비용 모두가 상당히 절약된다
- 단, 이동할때 서비스 유형에 따라 시간 및 리소스 측면에서 다양한 수준의 노력과 비용이 발생하므로 어느것이 효율성을 높일 수 있는 건지 확인해야한다