



Azure 서비스, 인증부터 다시 보자!

윈도 가상 데스크탑, 쿠버네티스 등등..



최영락 (Ian Choi)

마이크로소프트

Developer Product Marketing Manager

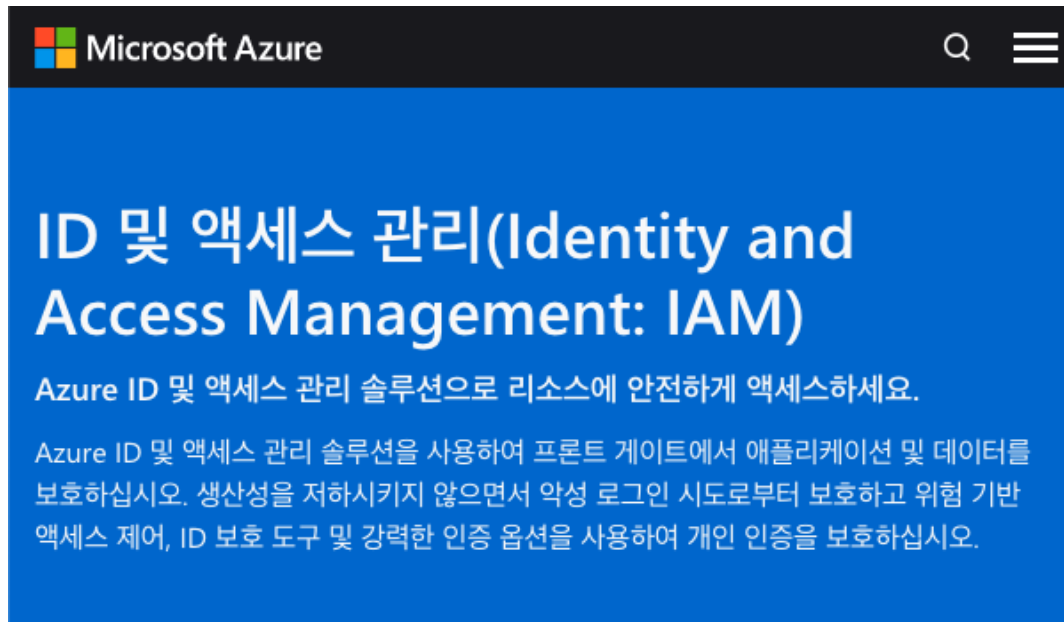
커뮤니티 활동

#DevCSeoul, #OpenStack

#K8sDocsL10nKorean, ...



IAM이라 불리는 클라우드 인증



먼저, 인증에 대해 잠깐 생각해 봅시다

“인증”이라는 단어만으로 파악하기 어려운 참뜻

Authentication (인증? 입증? 증명?)

Authorization (인증? 허가? 인가? 권한부여?)

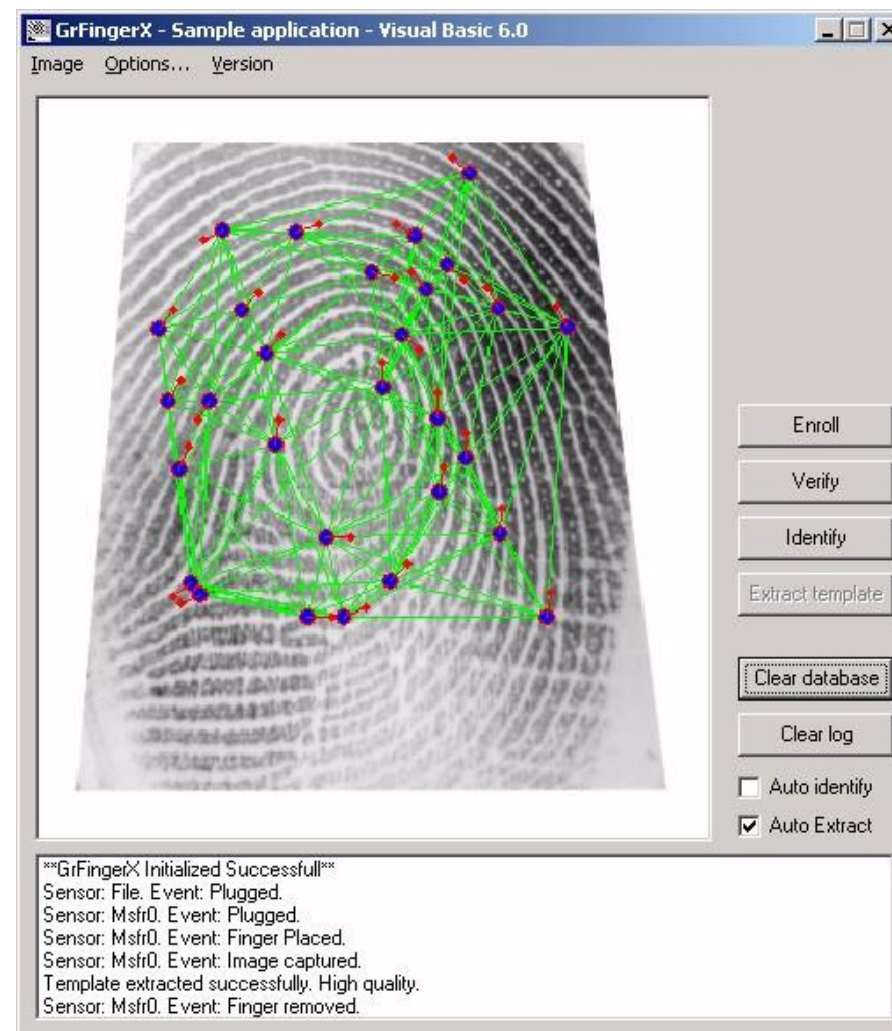
Identity (신원? 신분? 인증?)

Certification (자격증? 인증?)

Compliance (인증? 준수? 승인?)

오늘은 Authentication와 Identity쪽에 초점을 맞추고자 합니다.

암호화를 활용하는 방식



인증에 대한 짧은 히스토리 - (2)

인터넷, 나아가 "원격" 세상으로 오면서 더 중요해진 인증 체계

SSO (싱글 사인 온, Single Sign-On)

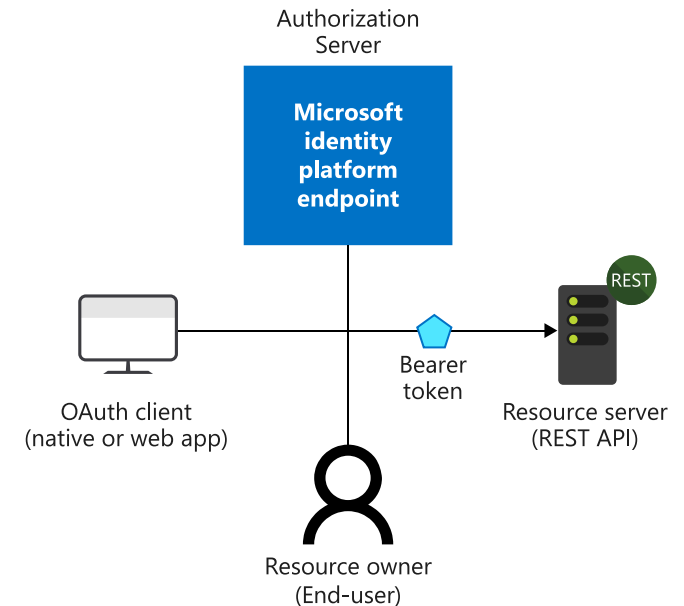
2차 인증을 넘는 다중 인증 체계 (Two/Multi-Factor Authentication)

OAuth, OpenID Connect, ...

OAuth 2.0 및 Microsoft ID 플랫폼에서 OpenID 연결 프로토콜

2020. 04. 13. • 읽는 데 3분 • 🍷 🍷 🍷 🍷

업계 표준 프로토콜인 OpenID Connect 및 OAuth 2.0을 사용한 서비스로서의 ID를 위한 Microsoft ID 플랫폼 엔드 포인트입니다. 서비스는 표준을 준수하지만 이러한 프로토콜의 두 구현 간에는 약간의 차이가 있을 수 있습니다. 여기에 있는 정보는 [오픈 소스 라이브러리](#) 중 하나를 사용하는 대신 HTTP 요청을 직접 전송 및 처리하여 코드를 작성하거나 타사 오픈 소스 라이브러리를 사용하도록 선택한 경우에 유용합니다.



(퍼블릭) 클라우드에서의 인증

1. 제공되는 자원에 대한 세부적인 접근 (엑세스) 권한 부여
2. 보안 제어 정책 적용
3. 모니터링, 감사 및 추적 기능
4. 기업에서 사용 중인 인증 체계와 통합

Azure에서의 IAM, Azure Active Directory!



Azure에서의 IAM, 얼레? 어디있지?!



The screenshot shows the Azure portal search interface with the search term 'IAM'. The search results are divided into three main sections: Services (서비스), Resources (리소스), and Marketplace (Marketplace). The Services and Resources sections both show '결과를 찾을 수 없습니다.' (No results found). The Marketplace section lists several products, with 'AXS GUARD Firewall - VPN - WAF - IAM for Azure' highlighted. Below the Marketplace section, there is a '설명서' (Documentation) section with links to Microsoft Docs articles about RBAC and Azure roles. At the bottom, the '리소스 그룹' (Resource Group) section also shows '결과를 찾을 수 없습니다.'

서비스 —————
결과를 찾을 수 없습니다.

리소스 —————
결과를 찾을 수 없습니다.

Marketplace ————— 모두 보기

- AXS GUARD Firewall - VPN - WAF - IAM for Azure
- Magento on Ubuntu powered by IAANSYS
- IBM QRadar SIEM v7.3.3 (BYOL)
- CloudXtream cDVR

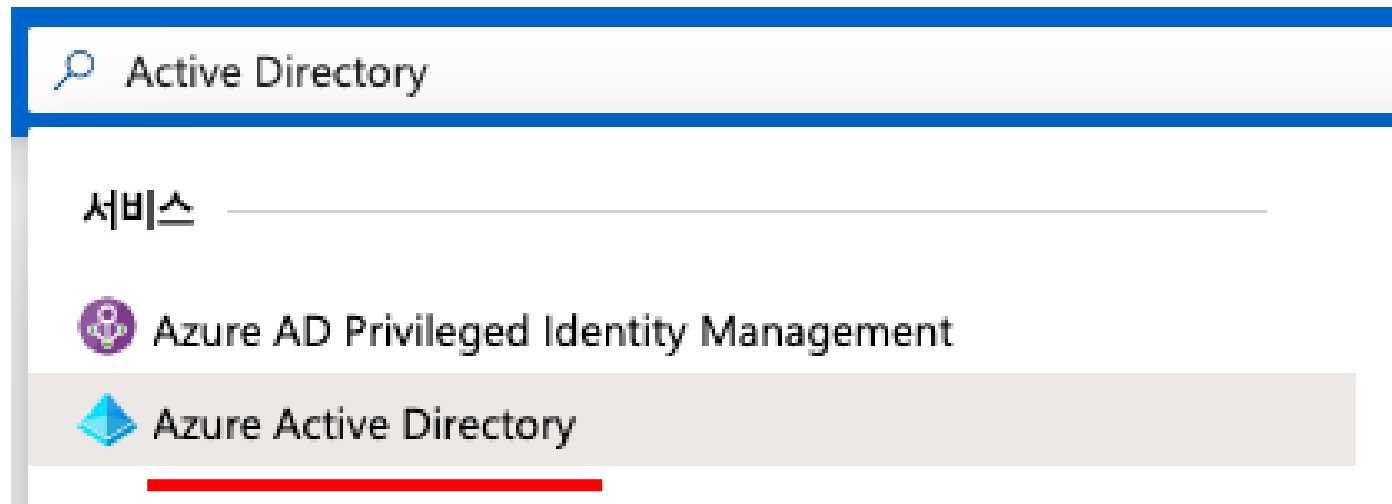
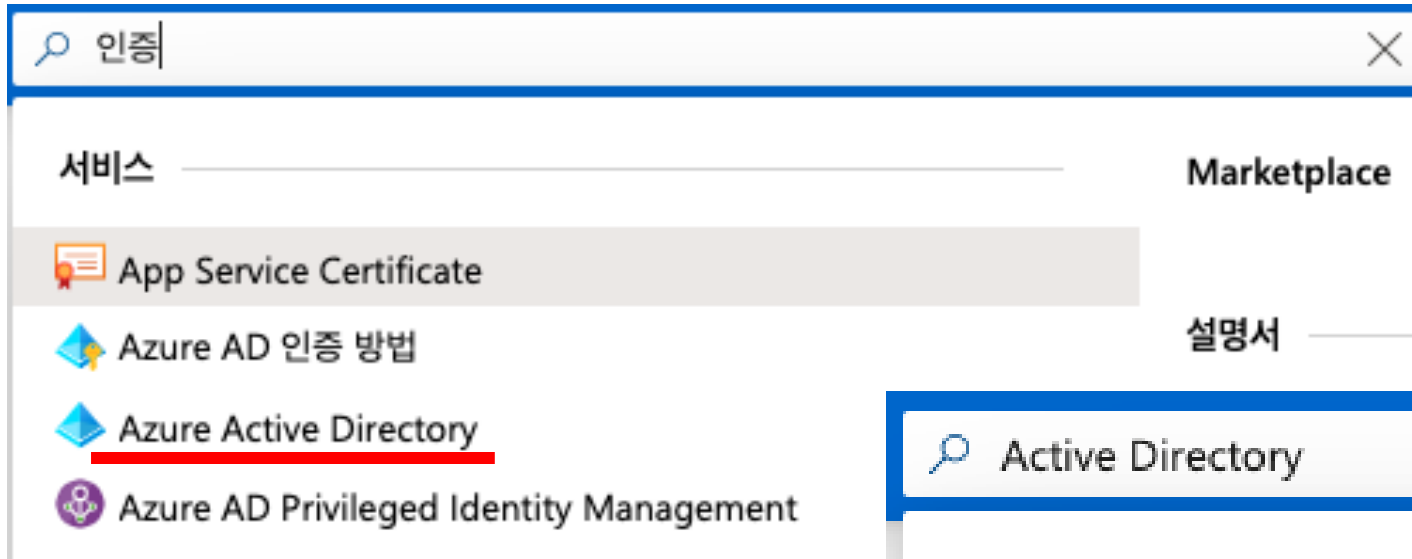
설명서 ————— 모두 보기

- [RBAC 및 Azure 포털을 통해 역할 할당 추가 또는 제거 | Microsoft Docs](#)
- [클래식 구독 관리자 역할, Azure RBAC 역할 및 Azure AD 역할 | Microsoft Docs](#)
- [Azure 리소스에 대한 RBAC\(역할 기반 액세스 제어\)란? | Microsoft Docs](#)
- [Azure 구독 관리자 추가 또는 변경 | Microsoft Docs](#)

리소스 그룹 —————
결과를 찾을 수 없습니다.

("IAM"으로 검색하면 잘 안 나옵니다...)

"Active Directory", "인증"으로 검색하세요



정말 인증에 대한 부분, 맞는 거 같죠? 😊



홈 > Default Directory | 개요

Default Directory | 개요

Azure Active Directory

개요

시작

문제 진단 및 해결

관리

- 사용자
- 그룹
- 조직 관계
- 역할 및 관리자(미리 보기)
- 관리 단위(미리 보기)
- 엔터프라이즈 애플리케이션

- 디바이스
- 앱 등록
- Identity Governance
- 애플리케이션 프록시
- 라이선스
- Azure AD Connect
- 사용자 지정 도메인 이름
- 모바일(MDM 및 MAM)
- 암호 재설정
- 회사 브랜딩
- 사용자 설정

사용자 | 모든 사용자(미리 보기)

Default Directory - Azure Active Directory

모든 사용자(미리 보기)

- 삭제된 사용자
- 암호 재설정
- 사용자 설정
- 문제 진단 및 해결

활동

- 로그인
- 감사 로그
- 대량 작업 결과

+ 새 사용자 + 새 게스트 사용자

이름

<input type="checkbox"/>	AR	aro
<input type="checkbox"/>	IY	Ian Y. Choi
<input type="checkbox"/>	WA	WVD Admin

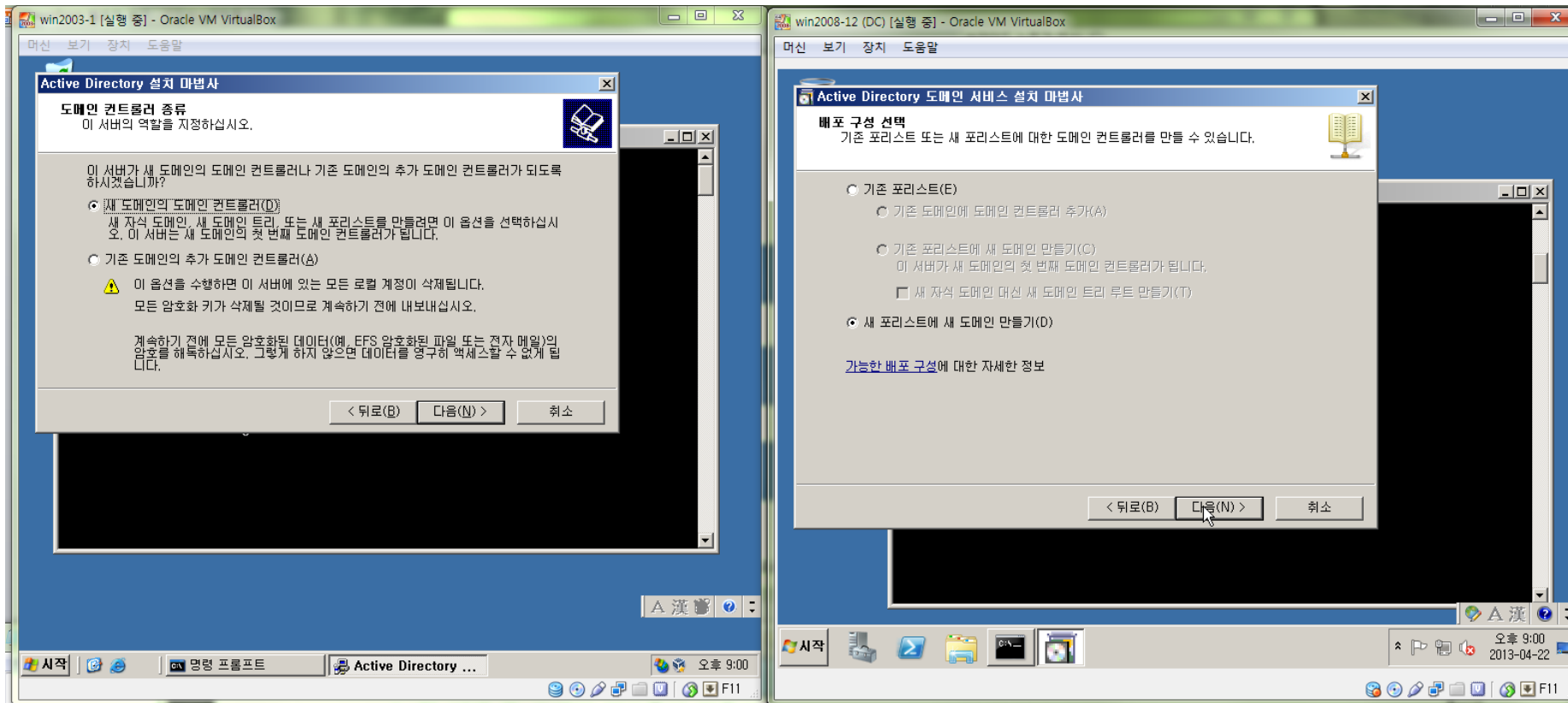
Azure Active Directory, 영상으로도 만나봅시다



네트워크 장벽이 허물어지고 있고,

IAM이 아닌, Azure Active Directory 이름으로 왜?

(윈도 서버, 그 전신은 NT부터 쓰이던 Active Directory라는 이름에서..)



Azure Active Directory, 어떻게 쓰일까요?

- 쿠버네티스 서비스 (Azure Kubernetes Service)



쿠버네티스 (Kubernetes) 소개 – (1)

Kubernetes: “컨테이너화된 응용 프로그램에 대한 자동화된 배포, 확장, 그리고 관리를 위한 오픈 소스 소프트웨어”

그리스어로 κυβερνήτης 입니다 – 배에 있는 키잡이 (Helmsman)를 의미합니다.

Docker 컨테이너가 항구/해안을 테마로 했던 것과 비슷하게,
Kubernetes는 컨테이너가 실어지는 배 운항을 담당하는 항해사를 테마로 합니다..

쿠버네티스 (Kubernetes) 소개 – (2)

History (짧은 역사)

Google에서 Borg를 오픈 소스화 + 지속적인 기여 중

Kubernetes v1.0: 2015년 7월 21일 릴리즈 (Founder: Joe Beda, Brendan Burns, Craig McLuckie)

GitHub를 메인 저장 공간으로 사용 중. 기여자: >1,700;

매 3-6개월마다 릴리즈 중

Kubernetes 관련 자세한 배경 & 아이디어:

[Large-scale cluster management at Google with Borg](#) 논문 참고

Azure Kubernetes Service (AKS)

오픈 소스 Kubernetes 사용 & 운영을 직접 Microsoft에서 "관리"




Microsoft Azure

홈 > 새로 만들기 > Kubernetes Service

Kubernetes Service

Microsoft



Kubernetes Service

Microsoft

[만들기](#)

Overview - Kubernetes Dashboard

127.0.0.1:8001/#!/overview?namespace=default

kubernetes

Search

+ CREATE

Overview

Cluster

- Namespaces
- Nodes
- Persistent Volumes
- Roles
- Storage Classes

Namespace

default

Overview

Workloads

Cron Jobs

Daemon Sets

Deployments

Jobs

Pods

Replica Sets

Replication Controllers

Stateful Sets

Discovery and Load Balancing

- Ingresses
- Services

Config and Storage

Config Maps

Workloads Statuses

Deployments: 100.00%

Pods: 100.00%

Replica Sets: 100.00%

Deployments

Name	Labels	Pods	Age	Images
gs-spring-boot-docker	run: gs-spring-boot-docker	1 / 1	22 hours	ianaksspringwinregistry.azurecr.io/gs-...

Pods

Name	Node	Status	Restarts	Age
gs-spring-boot-docker-7c6c4cddc5-jvbmj	aks-nodepool1-12766016-0	Running	0	22 hours

Replica Sets

Name	Labels	Pods	Age	Images
gs-spring-boot-docker-7c6c4cddc5	pod-template-hash: 7c6c4cddc5 run: gs-spring-boot-docker	1 / 1	22 hours	ianaksspringwinregistry.azurecr.io/gs-...

Azure 서비스, 인증부터 다시 보자!

이 때, Azure Active Directory, 인증은 어떤 관련이?

서비스 주체, 무엇일까요?



홈 > 새로 만들기 > Kubernetes Service > Kubernetes 클러스터 만들기

Kubernetes 클러스터 만들기

기본 사항 크기 조정 인증 네트워킹 모니터링 태그 검토 + 만들기

클러스터 인프라 서비스 주체는 Kubernetes 클러스터에서 클러스터에 연결된 클라우드 리소스를 관리하는 데 사용됩니다. [AKS의 서비스 주체에 대한 자세한 정보](#)

인증 및 권한 부여는 Kubernetes 클러스터에서 클러스터에 대한 사용자 액세스 및 사용자가 인증된 경우 수행할 수 있는 작업을 제어하는 데 사용됩니다. [Kubernetes 인증에 대한 자세한 정보](#)

클러스터 인프라

서비스 사용자 * ⓘ

(새) 기본 서비스 사용자

[내 서비스 사용자 구성](#)

Kubernetes 인증 및 권한 부여

RBAC(역할 기반 액세스 제어) ⓘ

아니요 **예**

내 서비스 사용자 구성

서비스 사용자

☐ 새로 만들기 ☒ 기존 항목 사용

서비스 사용자 클라이언트 ID * ⓘ

서비스 사용자 클라이언트 암호 * ⓘ

Configure service principal

Service principal

☐ Create new ☒ Use existing

Service principal client ID * ⓘ

559513bd-0c19-4c1a-87cd-851a26afd5fc ✓

Service principal client secret * ⓘ

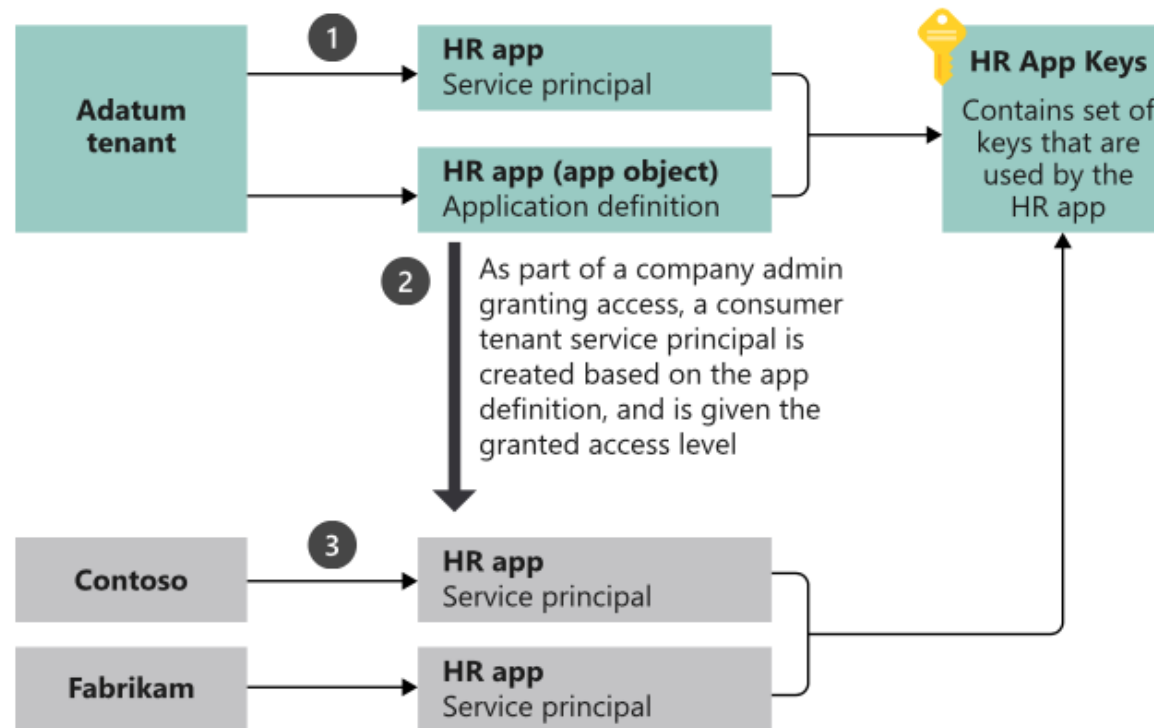
..... ✓

서비스 주체 (Service Principals)

특정 Azure 리소스에 액세스하기 위해 사용자 앱, 서비스, 자동화 도구에서 사용하는 보안 ID

다음 다이어그램은 **HR 앱**이라는 샘플 다중 테넌트 애플리케이션의 컨텍스트에서 애플리케이션의 애플리케이션 개체와 해당 서비스 주체 개체를 보여 줍니다. 이 예제 시나리오에는 다음 세 가지 Azure AD 테넌트가 있습니다.

- **Adatum** - HR 앱을 개발한 회사에서 사용하는 테넌트
- **Contoso** - HR 앱의 소비자인 Contoso 조직에서 사용하는 테넌트
- **Fabrikam** - HR 앱의 또 다른 소비자인 Fabrikam 조직에서 사용하는 테넌트



Azure Kubernetes Service
등에 액세스 하기 위해
Azure Active Directory가
이해할 수 있는 보안 ID를
생성하여 사용

서비스 주체 (Service Principals) 생성 방법

(Azure CLI에서는..)

서비스 주체 만들기

[az ad sp create-for-rbac](#) 명령을 사용하여 서비스 주체를 만듭니다. 서비스 주체를 만드는 경우 사용하는 로그인 인증 유형을 선택합니다.

① 참고

계정에 서비스 주체를 만들 수 있는 권한이 없는 경우 `az ad sp create-for-rbac` 에서 "권한이 부족하여 작업을 완료할 수 없습니다."라는 오류 메시지를 반환합니다. 서비스 주체를 만들려면 Azure Active Directory 관리자에게 문의하십시오.

서비스 주체에 사용할 수 있는 인증 유형에는 암호 기반 인증 및 인증서 기반 인증의 두 가지 유형이 있습니다.

암호 기반 인증

인증 매개 변수가 없으면 임의로 만든 암호를 통한 암호 기반 인증이 사용됩니다.

Azure CLI

복사

사용해 보세요.

```
az ad sp create-for-rbac --name ServicePrincipalName
```

Azure Active Directory, 어떻게 쓰일까요?

- 윈도 가상 데스크탑



윈도 가상 데스크탑 (Windows Virtual Desktop, WVD) 소개

가장 최상의 데스크탑 경험을 가상으로 Azure에서 제공



멀티 세션으로 경험하는 Windows 10은
오직 Azure에서만 지원하고 있음



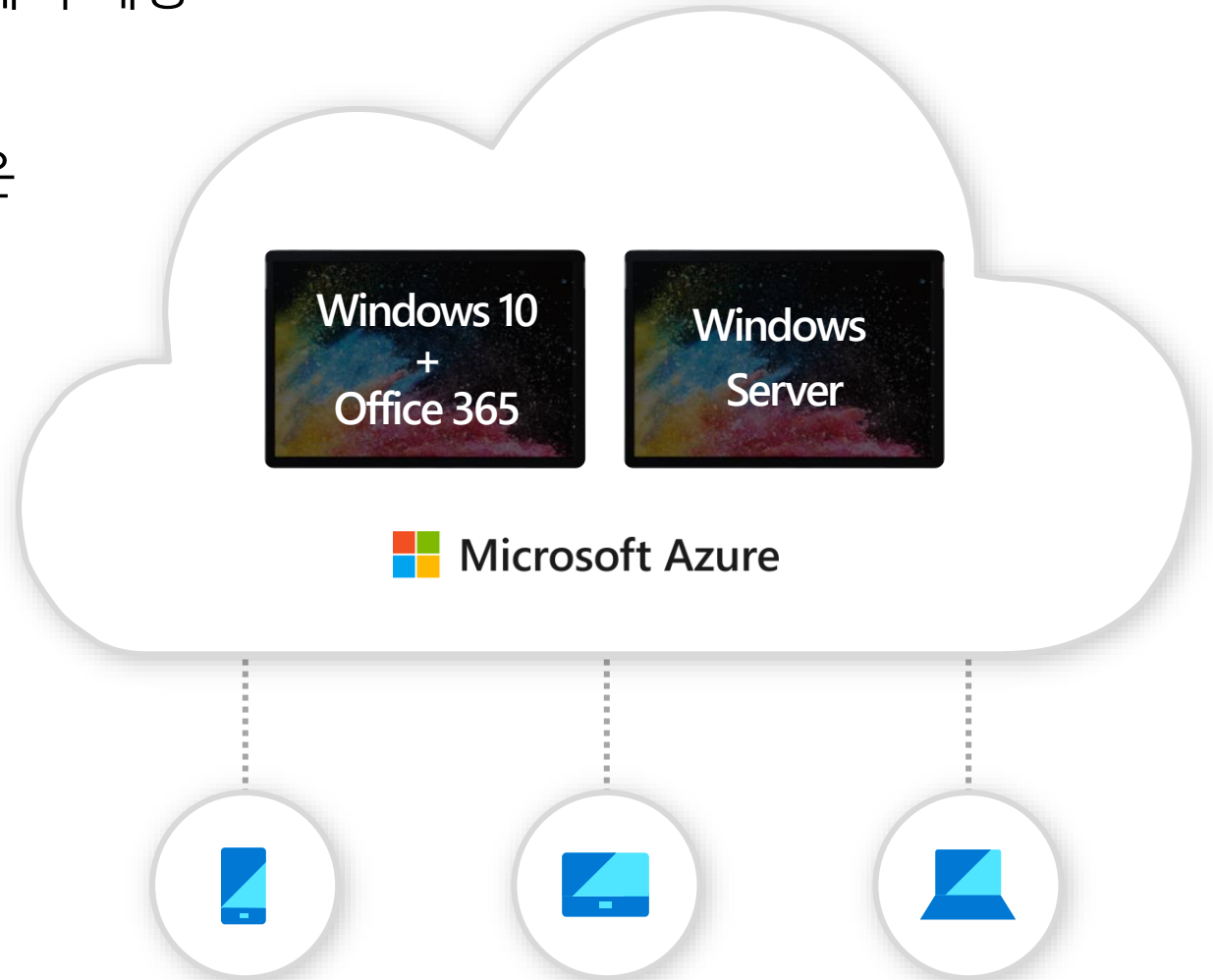
Office 365 ProPlus를
위한 최적화 활성화



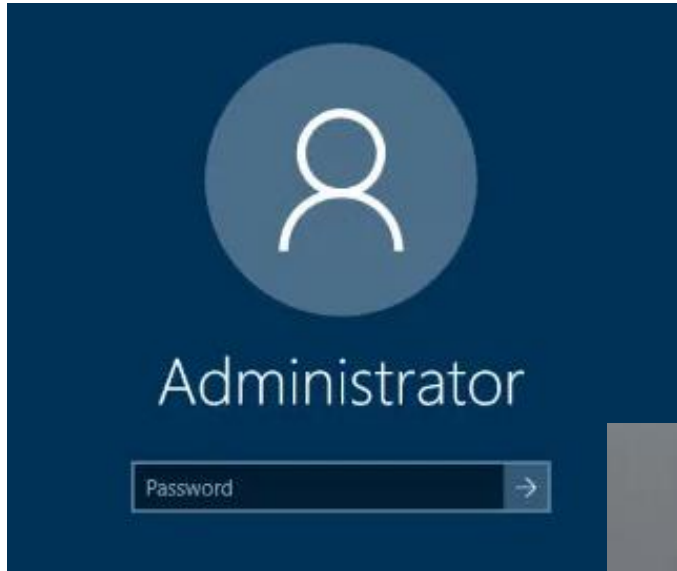
Windows Server (RDS)
데스크탑 및 앱 마이그레이션



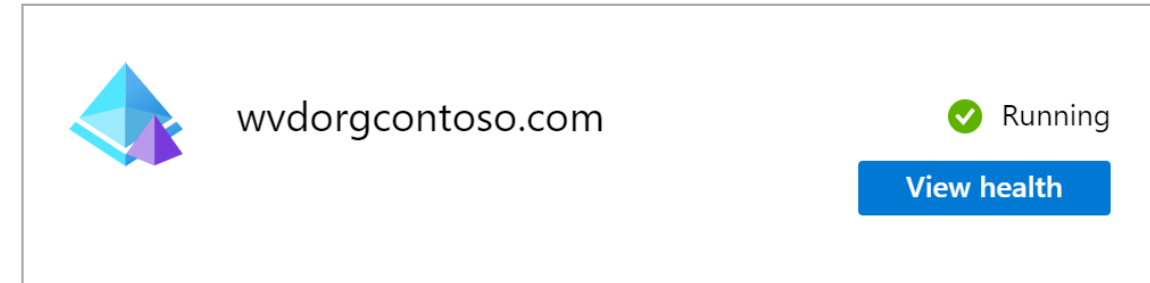
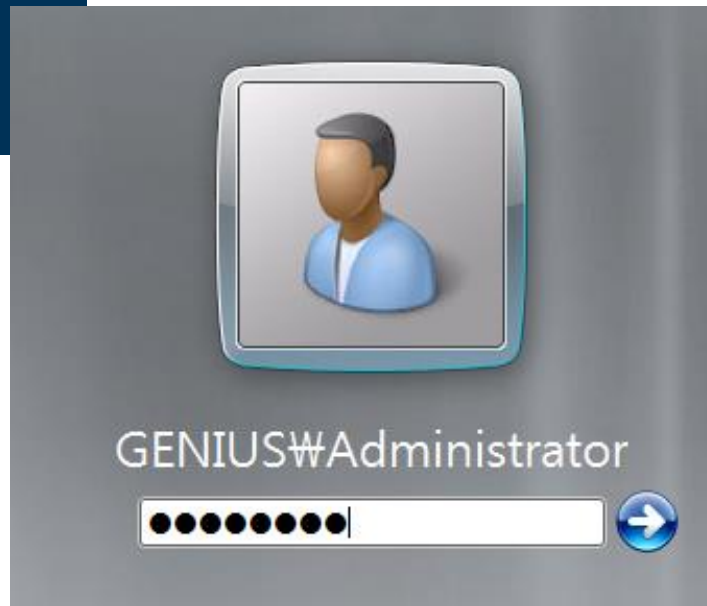
몇 분 안에 배포 & 스케일 가능



윈도 가상 데스크탑에서 인증이 왜 중요한가?



VS.



<input type="checkbox"/>	WA	wvd admin
<input type="checkbox"/>	WV	wvduser1
<input type="checkbox"/>	WV	wvduser2

윈도 가상 데스크탑, 설치 과정에서 인증을 보자

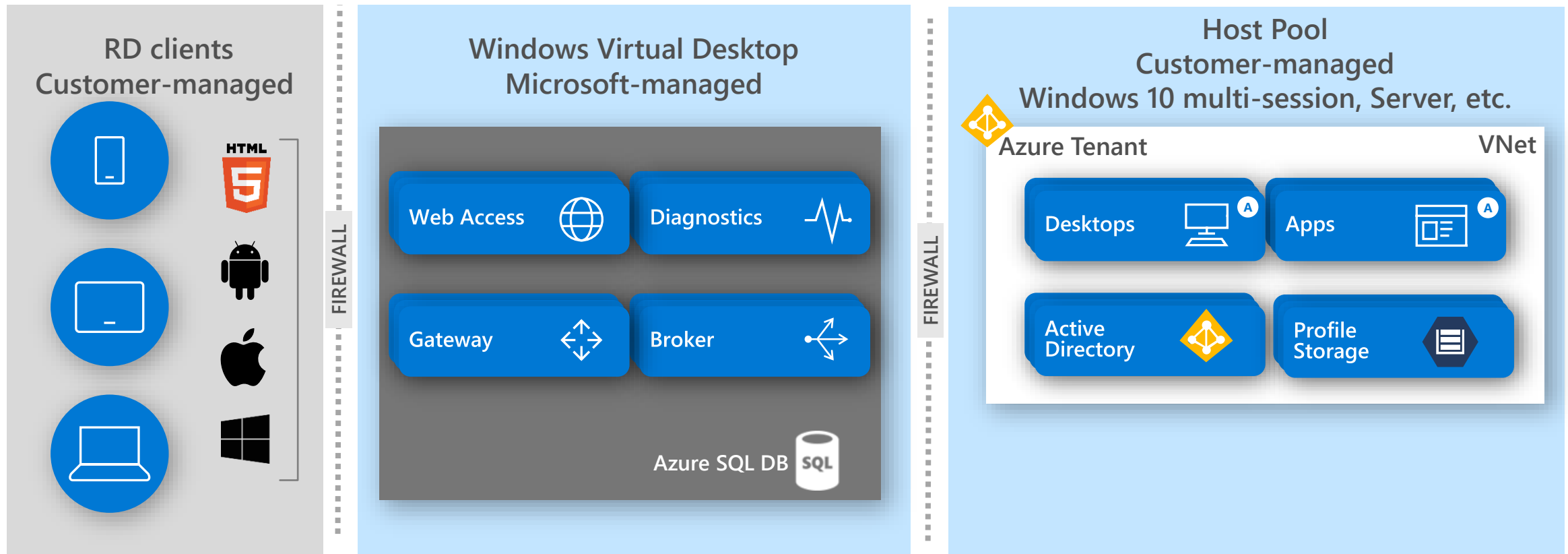


Identity (AD)

WVD Tenant
Consent & Creation

Host Pool Provision

Profile Storage



윈도 가상 데스크탑, Identity 전략 3가지



옵션



장점



단점

**Azure 구독에 있는 (기존)
도메인 컨트롤러 (DC)를 활성화**

VPN 또는 ExpressRoute가 온프레미스에 있는
경우 동기화 가능
친숙한 AD 그룹 정책 사용 가능
비용 감소를 위해 필요로 하는 경우 가상 머신
(일시)정지 가능

Azure에서 VM 및 Active Directory에 대한
부가적인 관리를 필요로 함

**클라우드를 기반으로 하는 조직의 경우,
Azure AD DS
(Active Directory Domain Services) 사용**

온프레미스와 따로 연결하지 않는 경우 또는
테스트 환경인 경우 사용하기 가장 좋음.
Azure AD 가 Identity에 대한 메인 소스가 됨.

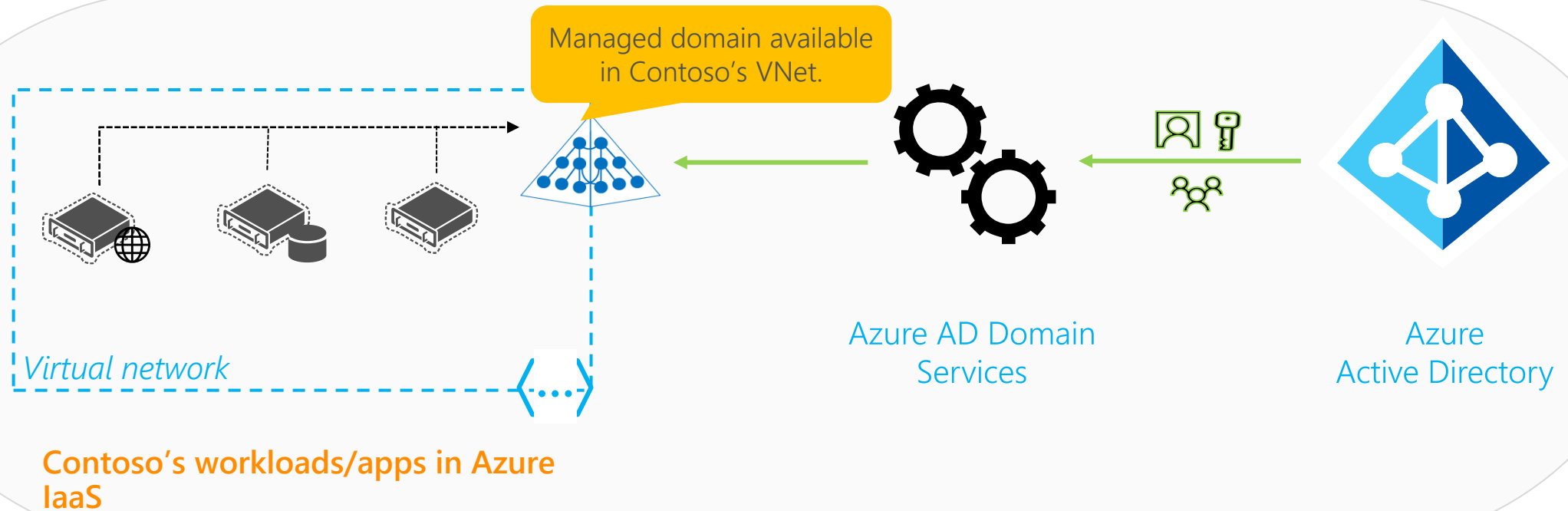
AD DS를 항상 구동해야 하므로 이에 따른
월별 고정 지출 발생

**하이브리드 조직의 경우, VPN 또는
ExpressRoute를 사용하며, Azure에
온프레미스를 위한 도메인 컨트롤러
(DC)가 있는 상황**

Azure에서 VM 및 Active Directory에 대한
부가적인 관리를 더해줌.
Azure에 AD DS 또는 도메인 컨트롤러를 필요로
하지 않음.

VM에 대한 사용자 인증에서 지연 (Latency)이
발생할 수 있음.
온프레미스 환경이 있다고 가정하고 있기에,
클라우드만을 위한 테스트 환경에 적합하지
않음.

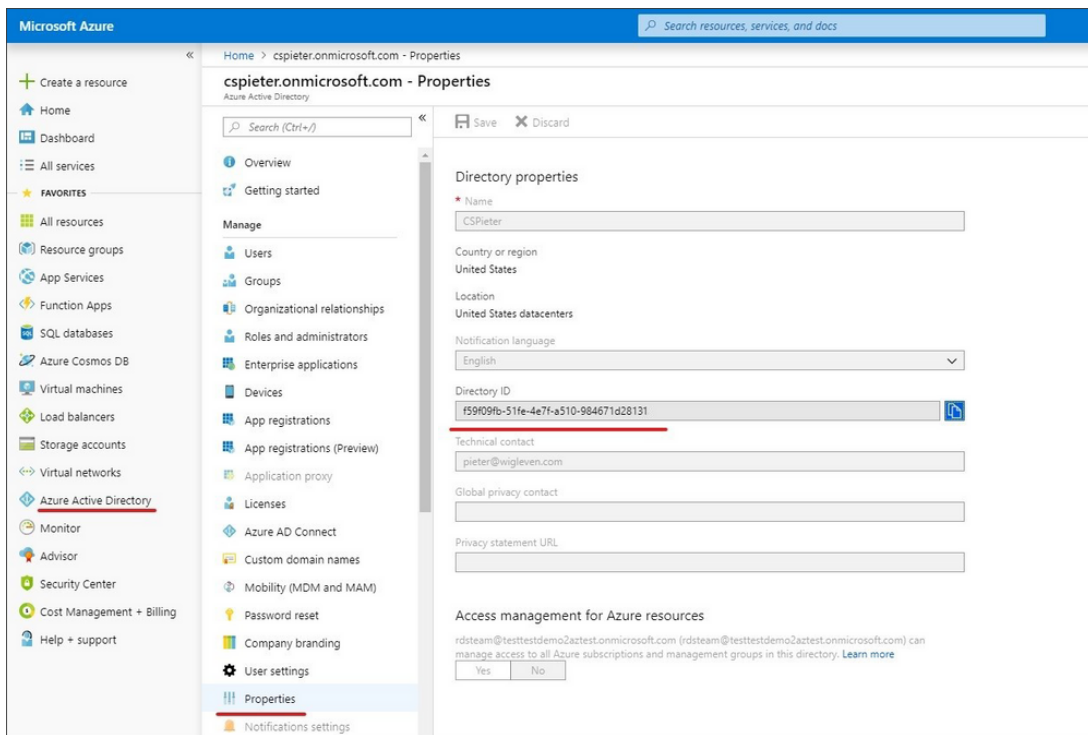
Azure AD Domain Services



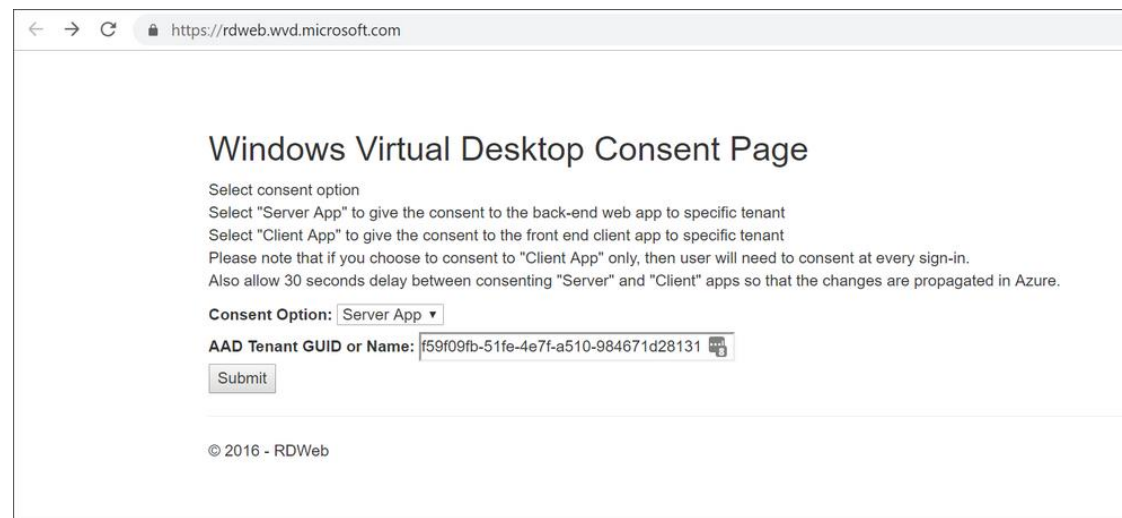
WVD 설치 단계: Azure AD 권한 관련



WVD 테넌트를 Azure 테넌트와 서로 연결

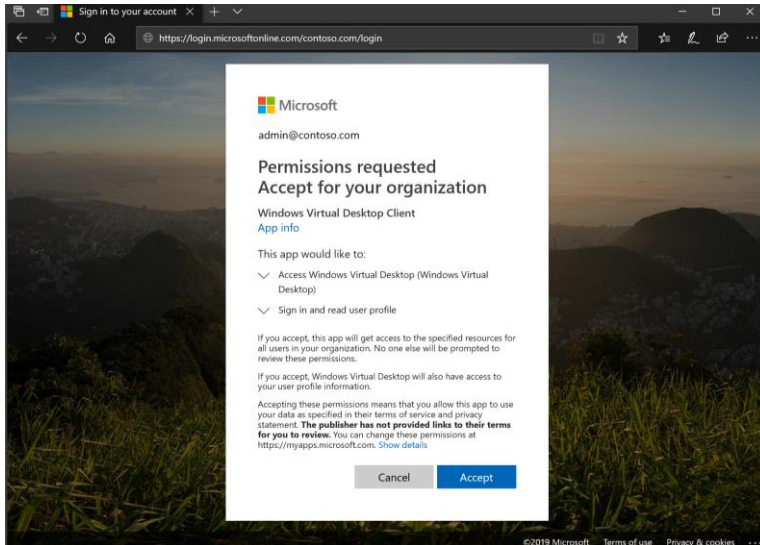


Azure AD 테넌트 ID

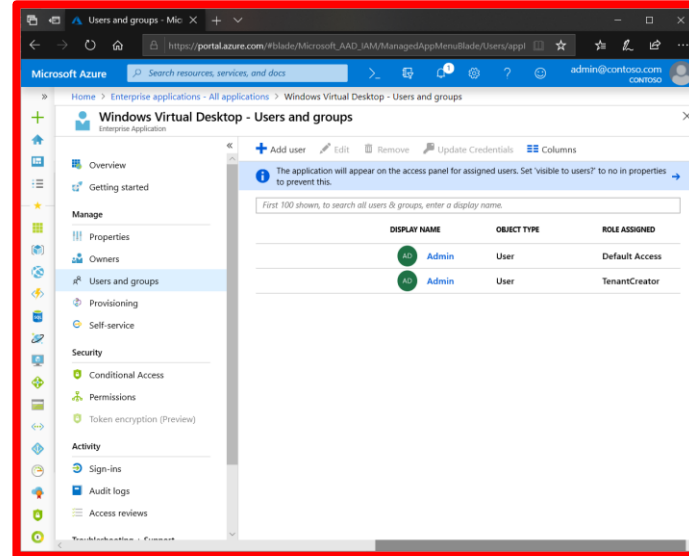


- <https://rdweb.wvd.microsoft.com>
- 접속 후 Azure AD 테넌트 ID 추가 및 디렉터리 ID 언급 후, **Submit (제출)**.

WVD 테넌트 프로비저닝 과정



- Azure AD consent 부여



TenantCreator 할당



테넌트 생성

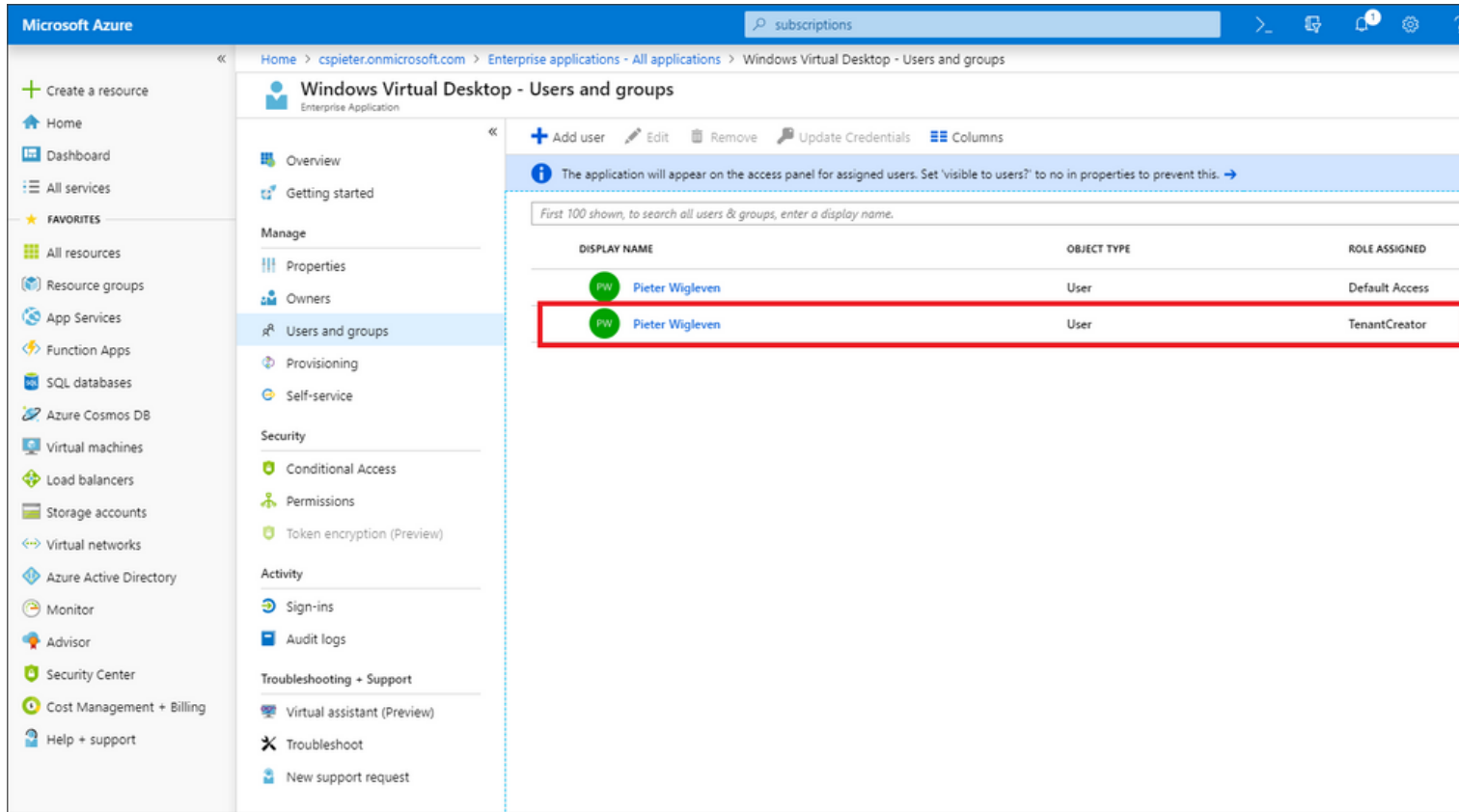
문서: aka.ms/wvdpreview

시작하기 가이드: aka.ms/startwvd

Azure 서비스, 인증부터 다시 보자!

#gav2020kr

“TenantCreator” 역할을 사용자 계정에 할당



- [Microsoft Azure 포털](#)에 로그인
- 왼쪽 메뉴 또는 검색에서 **Azure Active Directory** 를 찾기
- 메뉴 **Manage (관리)** → **엔터프라이즈 애플리케이션** 클릭
- **Windows Virtual Desktop** 찾아서 선택
- 관리에서 **사용자 및 그룹** 선택
- **사용자 추가** → **사용자 및 그룹**에서 윈도 가상 데스크톱 테넌트 생성을 수행하고자 하는 계정 사용자에게 권한을 할당/부여
- 선택 후 할당하면 “TenantCreator” 역할이 생성 됨

결론



마무리



1. Azure에서는 IAM == Azure Active Directory, 이것이 인증
2. Azure 퍼블릭 클라우드 내 사용자, 그룹, 권한 관리 모든 것이 가능
3. Azure 네이티브 서비스가 아닐 때, Azure와 인증 연동이 이루어져야 하며, 이를 위해 "서비스 주체"를 필요로 함 (예: AKS, ARO)
4. 통합 인증 관련 서비스 (예: WVD)의 경우 서비스 주체 뿐만 아니라, 테넌트 및 도메인 서비스 등 지식을 필요로 하기도 함.
5. Azure Active Directory는 윈도우 서버에서 언급하는 Active Directory와 다르나, 도메인 서비스에 대한 근본 개념은 궤를 같이 함.

당신의 목소리를 들려주세요!

Global Azure Virtual 2020는 여러분의 목소리를 기다립니다.
가감 없는 목소리가 발표자 분에게 매우 큰 힘이 됩니다.
앞으로 더 좋은 행사가 될 수 있도록 목소리를 내주세요.
감사합니다!

세션에 대한 목소리:

<https://sv.krazure.com/session-b3>

파트너사 행사:

<https://bit.ly/2RvJQzR>

