

9장

Azure SQL Database 및 Azure AD 사용하기

Azure SQL
Database
사용하기

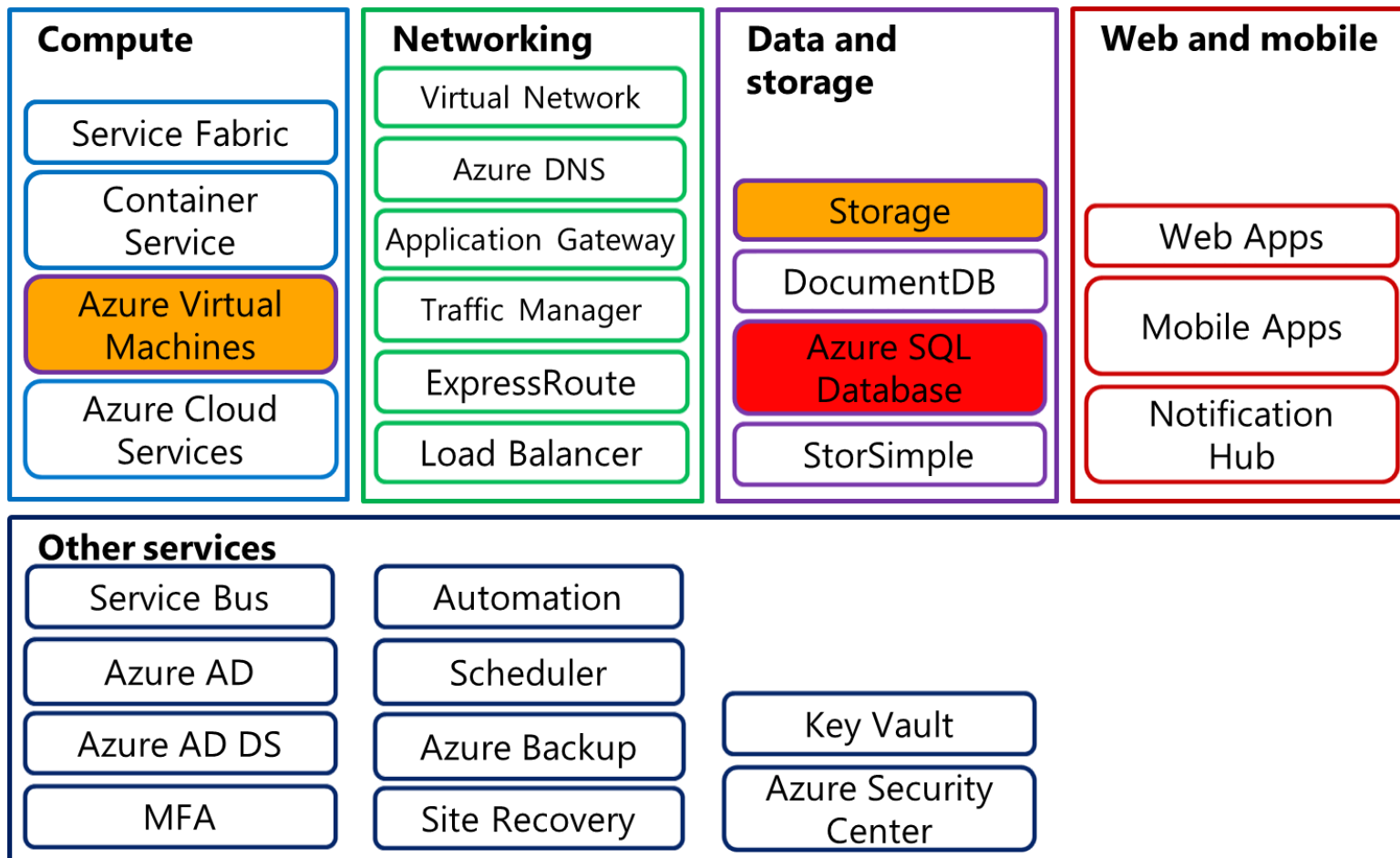
Azure Active
Directory
관리하기

1-Azure SQL Database 사용하기

- Azure SQL Database 소개
- Azure SQL Database 관리도구
- Azure에 SQL Database 생성하기
- SQL Server에 접속을 허용할 IP Address 지정하기
- SSMS로 SQL Server 관리하기
- Table 생성하기
- Azure SQL Database Login 및 User 생성하기
- sqlcmd 사용하기
- Geo-Replication 구성하기

1-Azure SQL Database 사용하기

- Azure SQL Database 소개
 - Relational database services as a component of Azure



1-Azure SQL Database 사용하기

특징	Azure SQL Database (PaaS)	SQL Server VM (IaaS)
Overhead (사내 VM과 비교하여)	최소	낮음 (Infra 지원 필요 없음)
Cost (사내 VM과 비교하여)	최소	낮음 (Infra 지원 필요 없음)
Provisioning time (사내 VM과 비교하여)	최소	낮음 (Infra 의존 없음)
Feature parity	No	Yes
Virtual network 지원	No	Yes
고가용성 및 확장성	Yes	Yes

** Azure SQL Database는 다음과 같은 기능(Feature)를 지원하지 않는다
(Distributed transactions, Service Broker, SQL Server Profiler feature,
Connectivity to OLE DB, Windows authentication)

1-Azure SQL Database 사용하기

- Azure SQL Database 소개
 - Azure SQL Database 배포 계획 옵션

Feature	Basic	Standard	Premium
최대 database size	2 GB	250 GB	500 GB-1 TB
DTU (Database Transaction Unit)	5	10-100	125-1750
Point-in-time restore	Any point in the last 7 days	Any point in the last 14 days	Any point in the last 35 days
Disaster recovery	Geo-restore, restore to any Azure region	Standard geo-replication; offline secondary	Active geo-replication; up to 4 online secondary backups
최대 in-memory OLTP storage	NA	NA	1 GB-10 GB
최대 동시 요청	30	60-200	200-2400
최대 동시 로그인	30	60-200	200-2400
최대 세션	300	600-2400	2400-32000

1-Azure SQL Database 사용하기

- Azure SQL Database 관리도구
 - Azure portal
 - Azure PowerShell module
 - Azure CLI
 - Azure Resource Manager templates
 - SQL Server Management Studio (SSMS)
 - SQLCMD
 - Visual Studio

1-Azure SQL Database 사용하기

- SQL Database with SQL Server on Azure 생성하기

SQL Database

* Database name

myazuresqlldb

✓

* Subscription

Azure Pass

▼

* Resource group ⓘ

☒ Create new ☐ Use existing

RGSQL

✓

* Select source ⓘ

Blank database

▼

* Server

sqlmyazure (Japan East)

>

Want to use SQL elastic pool? ⓘ

☐ Yes ☒ Not now

* Pricing tier ⓘ

Standard S2: 50 DTU, 250 GB

>

* Collation ⓘ

SQL_Latin1_General_CP1_CI_AS

Server

+ Create a new server

No servers found

New server

* Server name

sqlmyazure

✓

.database.windows.net

* Server admin login

adminuser

✓

* Password

.....

✓

* Confirm password

.....

✓

* Location

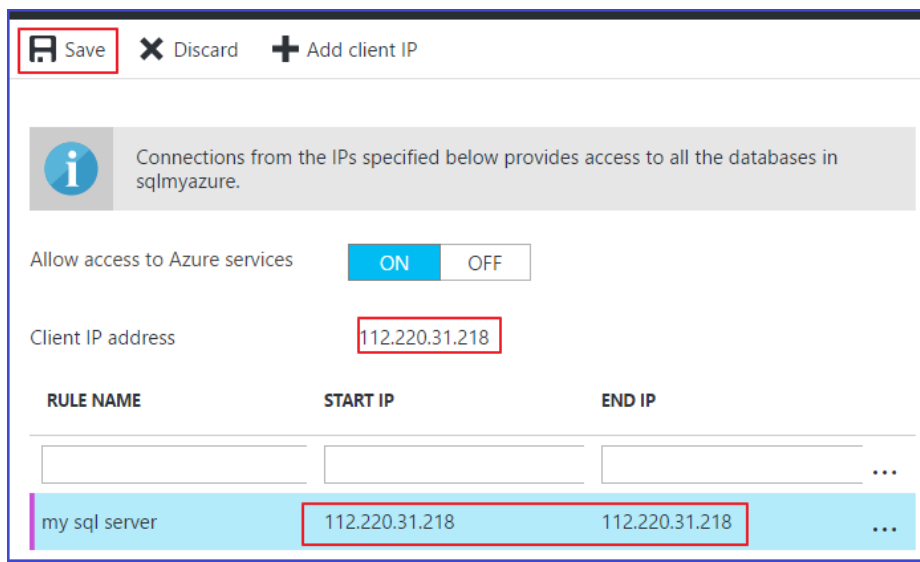
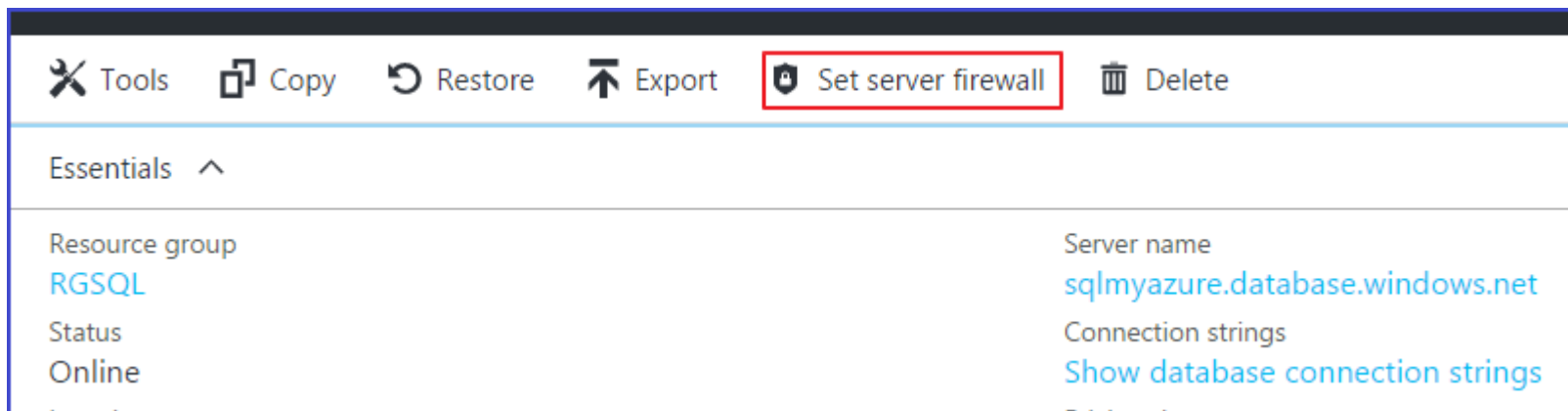
Japan East

▼

☒ Allow azure services to access server ⓘ

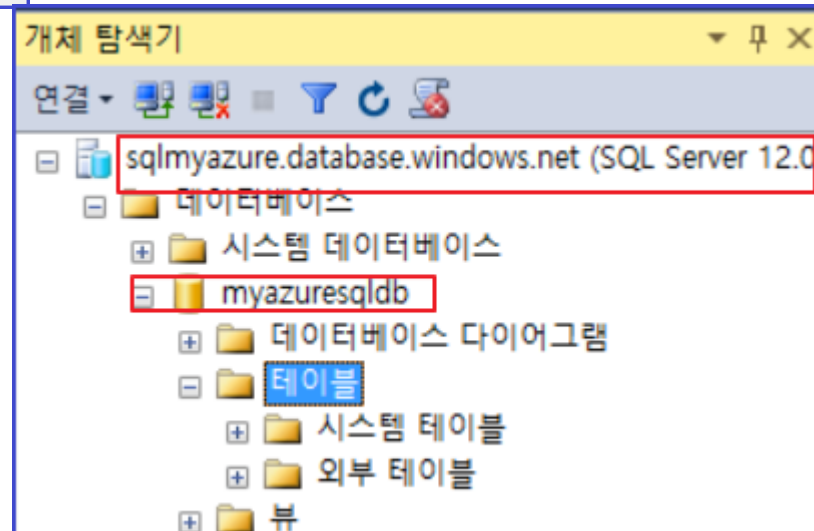
1-Azure SQL Database 사용하기

- SQL Server에 접속할 컴퓨터 지정하기
 - Firewall 설정으로 SSMS로 SQL Server를 관리하기 위해 접속하는 컴퓨터의 IP Address 허용하기



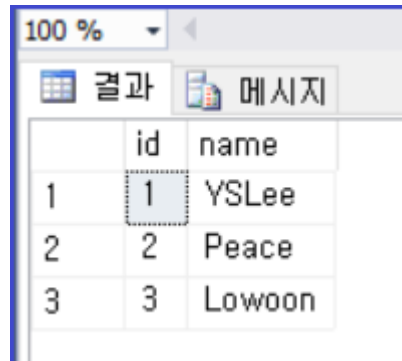
1-Azure SQL Database 사용하기

- SSMS를 사용하여 SQL Server에 접속하기
 - SQL Server의 fqdn을 알고 있어야 하며, SQL server 인증으로 접속한다



1-Azure SQL Database 사용하기

- Table을 생성하여 조회하기
 - CREATE TABLE tbl1 (id int, name varchar(8));
 - INSERT INTO tbl1 VALUES (1,'YSLEE');
 - INSERT INTO tbl1 VALUES (2,'Peace'),(3,"Lowoon");
 - SELECT * FROM tbl1;



100 %

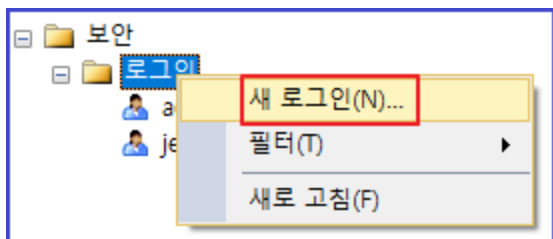
결과 메시지

	id	name
1	1	YSLee
2	2	Peace
3	3	Lowoon

1-Azure SQL Database 사용하기

- Azure SQL Server Login 생성하기

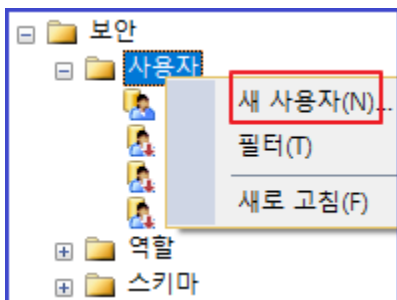
- jesuswithme라는 사용자가 Azure SQL Server에 로그인 할 수 있도록 Login 사용자 생성하기



```
CREATE LOGIN jesuswithme  
WITH PASSWORD = 'P@ssw0rd1234'  
GO
```

- Azure SQL Database에 접속하는 User 생성하기

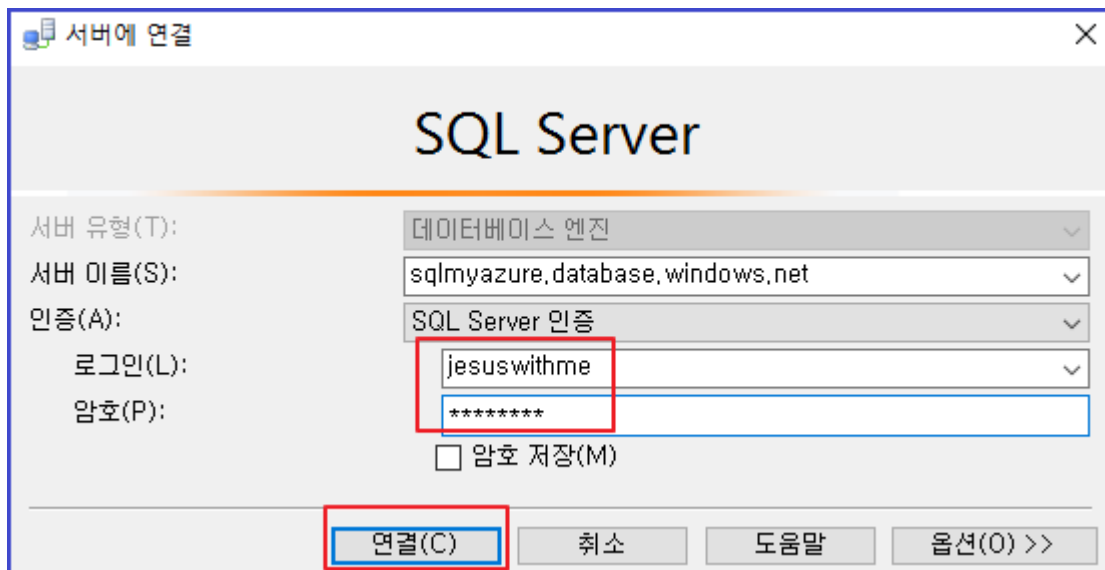
- 특정한 Database에 접속할 수 있는 User 생성하기



```
-- For login, create a user in the database  
CREATE USER jesuswithme  
FOR LOGIN jesuswithme  
WITH DEFAULT_SCHEMA = dbo  
GO  
-- Add user to the database owner role  
EXEC sp_addrolemember 'db_datareader', 'jesuswithme';  
GO  
EXEC sp_addrolemember 'db_datawriter', 'jesuswithme';  
GO
```

1-Azure SQL Database 사용하기

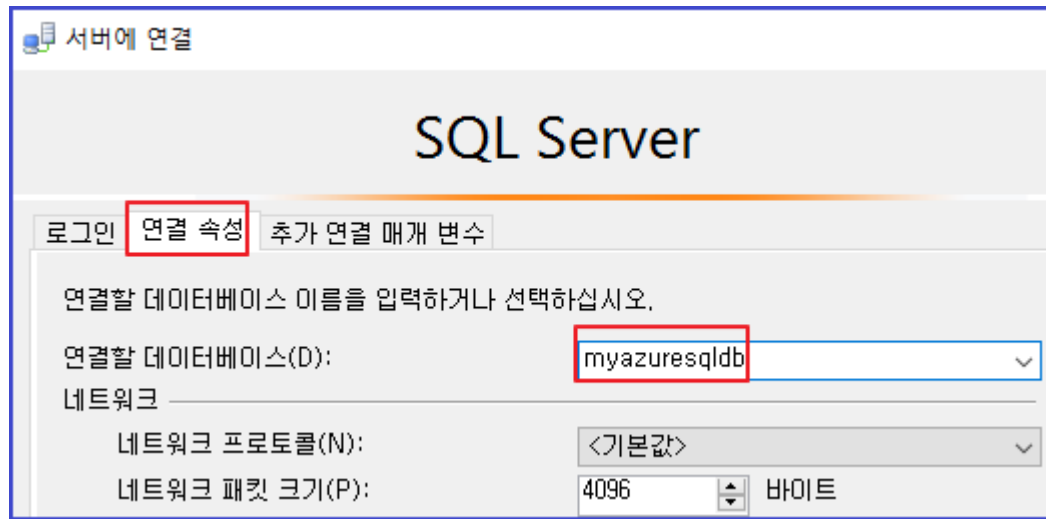
- 생성한 사용자 계정으로 SSMS로 Azure SQL Database에 접속



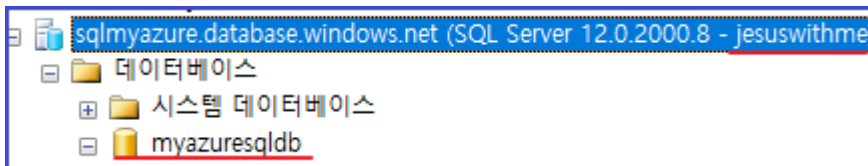
- 연결 실패
 - jesuswithme 계정이 접속할 Database를 지정하지 않았기 때문이다

1-Azure SQL Database 사용하기

- 생성한 사용자 계정으로 SSMS로 Azure SQL Database에 접속
 - "옵션"을 클릭하여 접속할 Database를 직접 입력한다



- 다시 연결을 시도한다
 - 연결 성공
 - jesuswithme 계정은 myazuresqladb의 모든 Table의 데이터를 읽기 및 저장 가능하다



1-Azure SQL Database 사용하기

- 생성한 사용자 계정으로 sqlcmd로 접속하기
 - **sqlcmd -S** sqlmyazure.database.windows.net **-d myazuresqlldb -U** jesuswithme
 - **SELECT @@version**
 - GO

```
-----  
Microsoft SQL Azure (RTM) - 12.0.2000.8  
Feb  8 2017 04:15:27  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
```

- **SELECT * FROM tbl1;**
- GO

```
1> SELECT * FROM tbl1;  
2> GO  
id          name  
-----  
1 YSLee  
2 Peace  
3 Lowoon  
  
(3개 행 적용됨)  
1> _
```

1-Azure SQL Database 사용하기

- Geo-Replication 구성하기

- Primary database를 원격 데이터센터에 있는 Secondary database에 주기적으로 복사하기
 - Standard edition: Secondary database is an offline redundant copy; only one copy is supported
 - Premium edition: Secondary databases are read-only
- Failover procedure:
 1. Bring the secondary database online
 2. Modify application connection strings

1-Azure SQL Database 사용하기

- Geo-Replication 구성하기
 - 가장 가까운 원격 데이터센터를 선택한다



1-Azure SQL Database 사용하기

- Geo-Replication 구성하기
 - Secondary type을 Readable로 하고 복사할 Azure SQL 서버를 생성한다

Create secondary

Create geo-replicated secondaries to protect against prolonged datacenter outages. Secondaries have price implications. [Learn more](#)

Region
Japan West

Database name
myazuresqldb

* Secondary type
Readable

* Target server
Configure required settings

Server

+ Create a new server

No servers found

New server

* Server name
myazuresqldbread

.database.windows.net

* Server admin login
adminuser

* Password
.....

* Confirm password
.....

* Location
Japan West

☒ Allow azure services to access server

1-Azure SQL Database 사용하기

- Geo-Replication 구성하기
 - Secondary Azure SQL Server에 Firewall 설정하여 접속 허용하기
 - More Services - SQL Server 검색 - 생성한 Secondary Server 선택(myazuresqldbread) - Firewall 선택한 후 아래와 같이 작업

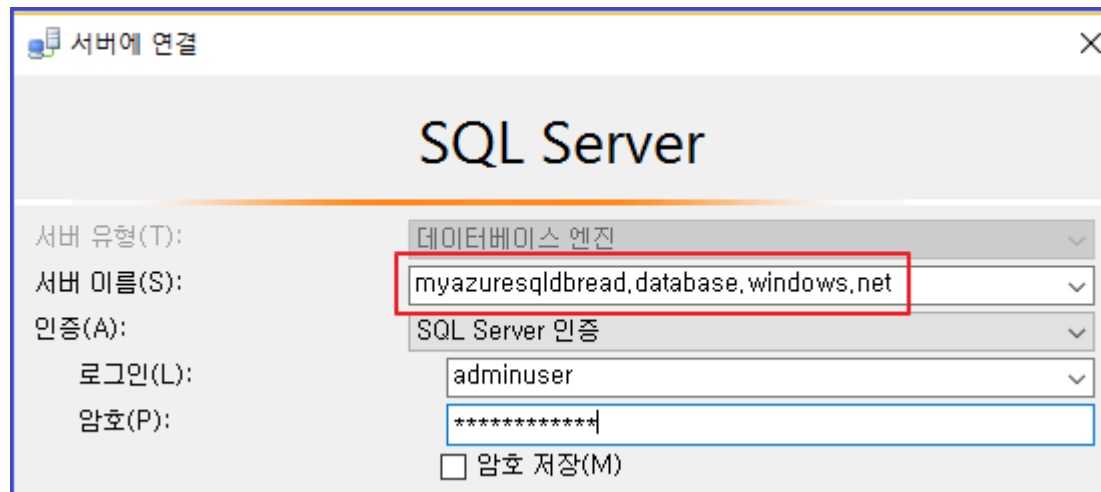
The screenshot shows the Azure Firewall configuration interface. At the top, there are three buttons: 'Save' (highlighted with a red box), 'Discard', and 'Add client IP'. Below this is an information banner with an 'i' icon and the text: 'Connections from the IPs specified below provides access to all the databases in myazuresqldbread.' Underneath the banner, there is a toggle switch for 'Allow access to Azure services' which is currently set to 'ON'. Below the toggle, the 'Client IP address' field contains the value '182.216.60.95' (highlighted with a red box). At the bottom, there is a table with three columns: 'RULE NAME', 'START IP', and 'END IP'. The first row of the table has the following values: 'my home' (with a green checkmark), '182.216.60.95' (with a green checkmark), and '182.216.60.95' (with a green checkmark). The entire table row is highlighted with a red box.

RULE NAME	START IP	END IP
my home ✓	182.216.60.95 ✓	182.216.60.95 ✓ ...

1-Azure SQL Database 사용하기

- Geo-Replication 구성하기

- SSMS에서 "연결"을 클릭하여 SQL database에 접속한다. 이 때 adminuser를 사용한다
- 접속할 컴퓨터 이름은 "Properties"를 클릭하면 알 수 있다



- 접속이 성공한 후에 조회 및 입력하는 T-SQL 구문을 실행한다
 - SELECT * FROM tbl1; (##성공)
 - INSERT INTO tbl1 VALUES (4,'HEART'); (##읽기 전용이어서 실패함)

2-Azure Active Directory 관리하기

- Azure AD 필요성
- Azure에서 AD를 이용하는 요소
- Azure Active Directory (AAD) 소개
- Azure AD Premium 소개
- Azure AD를 이용한 관리 Portal들
- Azure Active Directory Edition별 세부 설명

2-Azure Active Directory 관리하기

- Azure AD 필요성

매일 10-20 억 인증

7백만 개 조직

2,477 2,532 개
SaaS 앱 & Office 365와
SSO

5.20억 Identity

Azure에서 AD를 이용하는 요소

Compute

Service Fabric

Container
Service

Azure Virtual
Machines

Azure Cloud
Services

Networking

Virtual Network

Azure DNS

Application Gateway

Traffic Manager

ExpressRoute

Load Balancer

Data & Storage

Storage

DocumentDB

Azure SQL
Database

StorSimple

Web & Mobile

Web Apps

Mobile Apps

Notification
Hub

Other services

Service Bus

Azure AD

Azure AD DS

MFA

Automation

Scheduler

Azure Backup

Site Recovery

Key Vault

Azure Security
Center

Azure Active Directory (AAD) 소개

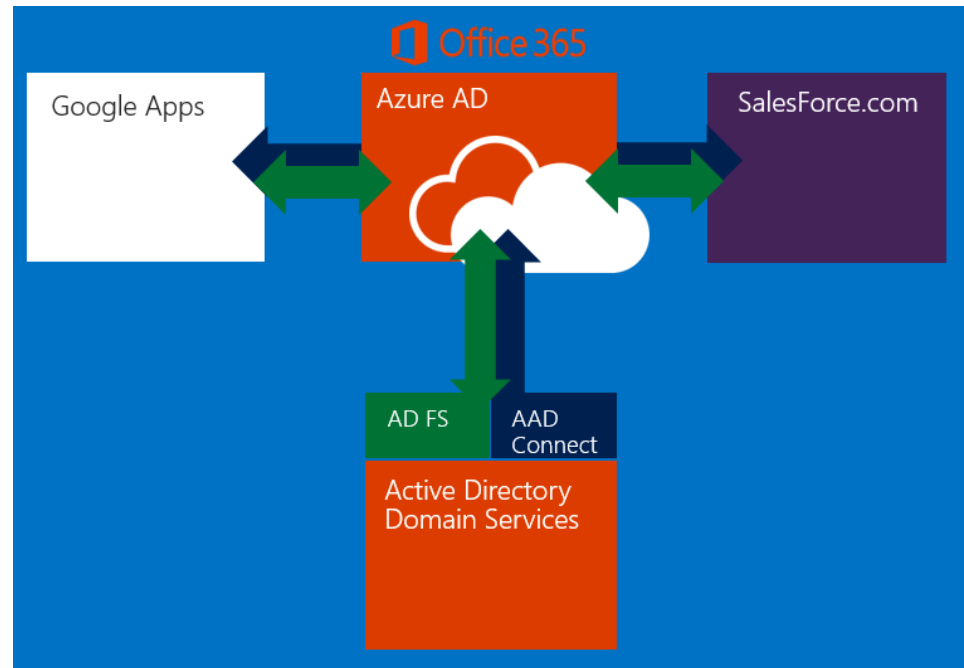
- AAD는 MS 온라인 서비스를 위한 Identity 플랫폼 역할
 - 인증을 제공하고 아래 서비스를 위한 디렉터리 정보 제공
 - Azure Cloud
 - Office 365 (Exchange Online, Skype Online, SharePoint Online)
 - Microsoft Intune
 - Dynamics Online
 - Azure RMS (AIP: Azure Information Protection)
 - 더 많은 서비스들이 추가될 예정...
- **Multiple cloud services** can use Azure AD for authentication and authorization:
 - **Azure**
 - **Office 365**
 - **Intune**

Azure Active Directory (AAD) 소개

- Azure AD 주요 특징
 - Microsoft가 직접 관리
 - Service로 제공하는 Platform이다
 - Multitenant 지원
 - User, Group, Application, device 지원
 - On-Premises AD에 비교하여 지원하지 않는 기능
 - OU와 Computer Object는 사용 못함
 - Group Policy 지원 안함
 - Forest 지원 안함 (하지만 Federation을 사용하여 인증과 권한 제공)
 - Role-Based Access Control(RBAC)을 사용하여 관리 위임
 - multi-factor authentication(MFA) 지원
 - 아래 것에 대하여 인증과 권한 제공:
 - Cloud identity
 - Synchronized identity
 - Federated identity

Azure Active Directory (AAD) 소개

- AAD is Identity Management as a Service
 - 클라우드의 Identity 서비스
 - 3rd party SaaS
앱을 위한 동기화와 SSO
 - 앱 액세스 패널
(myapps.microsoft.com)
 - 다단계 인증(MFA)
 - 셀프-서비스 암호 재설정

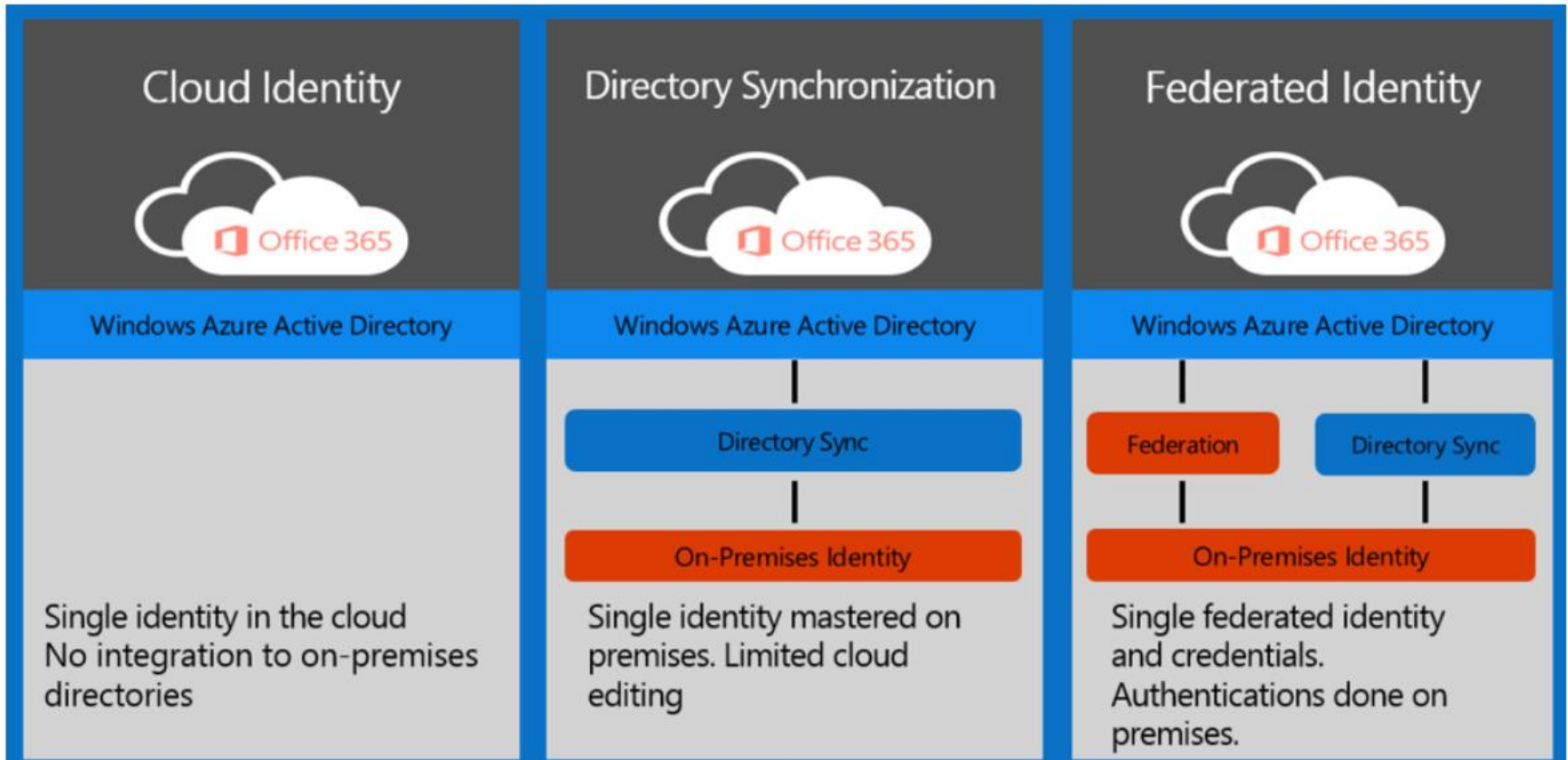


Azure Active Directory (AAD) 소개

- Azure AD Business to Business (B2B) 기능:
 - Provides simple and secure sharing of data and applications
 - Works with partners that have their own Azure AD tenant and with partners that do not have an Azure AD tenant
 - Requires a company to federate only once with Azure AD
- Azure AD Business to Business (B2C) 기능:
 - Provides Identity as a Service for applications
 - Supports standard protocols, such as OpenID Connect and OAuth 2.0
 - Supports identity management by using social accounts such as **Facebook, Google, and LinkedIn**

Azure Active Directory (AAD) 소개

- Azure AD의 핵심 시나리오



Azure Active Directory (AAD) 소개

• Azure AD의 핵심 시나리오



Azure AD Premium 소개

- AAD Premium의 주요 기능(Feature)
 - Self-service group management
 - Advanced security reports and alerts
 - Multi-Factor Authentication
 - Microsoft Identity Manager (MIM)
 - Enterprise SLA of 99.9 percent
 - Self-service password reset with writeback
 - Cloud App Discovery
 - Azure AD Connect Health

Azure AD Premium 소개

- AAD Premium에 액세스하기
 - 적절한 디렉터리에 적절한 구독이 필요
 - 전역 관리자(Global Admin)는 AAD Premium에 쉽게 액세스할 수 있다
 - Office 365 관리자 포털의 왼쪽 창에서 Azure AD 클릭
 - <http://aka.ms/accessaad>
 - 청구 관리자는 구독을 적절한 디렉터리에 연결해야 함
 - 계정 포털에서 구독이 올바른 디렉터리에 할당되었는지 확인

Azure AD를 이용한 관리 Portal들

- 각각의 Portal
 - Office 365
 - **portal.office.com**
 - Office 365에 초점, AAD Premium 기능 없음
 - Azure AD
 - **aad.portal.azure.com**
 - AAD Basic & Premium에 초점
 - AAD 포털에서만 제공되는 몇 가지 기능
 - SaaS 앱, 그룹 구성 또는 portal.azure.com
- Intune Portal
 - **manage.microsoft.com**
- CRM Portal
- PowerShell
- Graph API

Azure Active Directory Edition 별 세부 설명

기능	Azure AD (무료)	Azure AD Basic	Azure AD Premium
Directory as a Service	최대 500,000 개체	개체 제한 없음	개체 제한 없음
UI 혹은 PowerShell cmdlet을 통해 사용자와 그룹 관리	예	예	예
SaaS 및 사용자 정의 앱에 SSO 기반 사용자 액세스를 위한 액세스 패널 포털	사용자당 10개의 앱	사용자당 10개의 앱	제한 없음
사용자 기반 앱 액세스 관리/ <u>프로비저닝</u>	예	예	예
클라우드 사용자를 위한 <u>셀프</u> -서비스 암호 변경	예	예	예
디렉터리 동기화 도구 – 온- <u>프레미스</u> Active Directory와 Azure Active Directory간 동기화	예	예	예
표준 보안 리포트	예	예	예
<u>고가용성</u> SLA 가동 시간 (99.9%)		예	예
그룹 기반 앱 액세스 관리 및 <u>프로비저닝</u>		예	예
회사 <u>브랜딩</u> – 로그인/액세스 패널 페이지의 회사 로고와 색상에 대한 <u>커스터마이징</u>		예	예
클라우드 사용자를 위한 <u>셀프</u> -서비스 암호 재설정		예	예
Bring Your Own App (BYOA) 구성			예

AAD 에디션 <https://msdn.microsoft.com/en-us/library/azure/dn532272.aspx>

Office365+AAD <http://blogs.office.com/2015/02/17/sign-page-branding-cloud-user-self-service-password-reset-office-365>

Azure Active Directory Edition별 세부 설명

기능	Azure AD (무료)	Azure AD Basic	Azure AD Premium
Application Proxy		예	예
클라우드 사용자를 위한 <u>셀프</u> -서비스 그룹 관리		예	예
온- <u>프레미스</u> write-back을 제공하는 <u>셀프</u> -서비스 암호 재설정			예
MIM (Microsoft Identity Manager) 서버 라이선스 – 온- <u>프레미스</u> 데이터베이스와 디렉터리, Azure Active Directory간 동기화			예
고급 변칙 보안 리포트 (머신 러닝 기반)			예
고급 사용량 <u>리포팅</u>			예
클라우드 사용자를 위한 MFA 서비스			예
온- <u>프레미스</u> 사용자를 위한 MFA 서비스			예
Cloud App Discovery			예
Azure AD Connect Health			예