

.NET Conf

探索 .NET 新世界



Host by
STUDY4

特別感謝



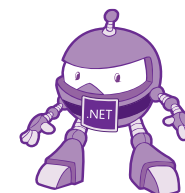
R-Ladies Taipei



多奇·數位創意



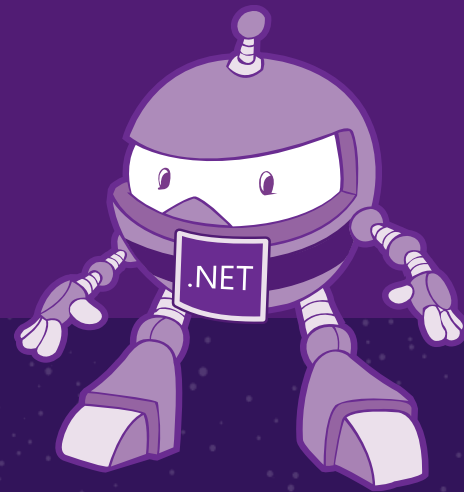
以及各位參與活動的你們



Azure App Service Security

Sky Chang
終身打雜 - 後端攻城獅

STUDY4.TW
為 學 習 而 生



Web Development

Study4.TW Study4Love

ALM DevOps Agile Scrum

DevDayAsia DotNetConf

skychang.github.io

TechDays Channel9

GitHub GitBook

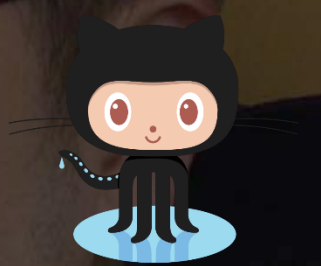
Global Azure Bootcamp

Premier Field Engineer

STUDY4.TW
為 學 習 而 生



天空的垃圾場
skychang.github.io



github.com/skychang

終生
後端攻城獅



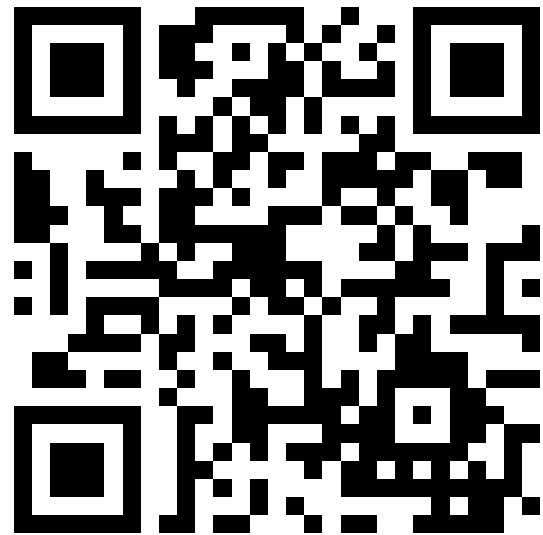
Web Development
Cloud & Azure
ALM & DevOps
Agile & Scrum

Sky.Chang@microsoft.com

Sky Chang

注意事項

- 結束後會提供投影片
- 原講師受傷開刀中，請大家祝她早日康復
- 想了解過程的可以參考
- <https://ppt.cc/fJT2ex>
- 祝大家都順利平安



Agenda

- App Service
- Managed identities for Azure resources
- Azure Key Vault
- Service Endpoints



Azure App Service

Quickly build, deploy and scale powerful cloud applications without worrying about infrastructure

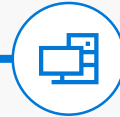
High productivity



.NET, Node, Java, Docker,
PHP, Ruby, Python



Staging &
deployment



Testing in
production



App gallery
marketplace

Fully managed



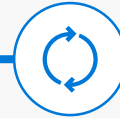
Auto scale &
load balancing



High availability
w/ auto patching



Reduced
operations costs



Backup &
recovery

Enterprise grade



Global data
center footprint



Hybrid
support



AAD
integration



Secure &
compliance

問題..

- 在地端可以很輕易地使用 Windows 驗證，那雲端呢？
 - App Service 要怎麼存取 SQL Database?
- 當使用 Key Vault 的時候，你的應用程式怎麼讓 Key Vault 知道你通過驗證授權？

Managed identities for Azure resources



Managed identities for Azure resources

- 前名稱為 受控服務識別 (MSI)
 - Managed Service Identity
- Azure 資源適用受控識別
 - Managed identities for Azure resources
- 免費、免費、免費

Managed identities for Azure resources

- 用戶端識別碼

- Azure AD 所產生的唯一識別碼，初始化時，會繫結 Service 和 SP

- 主體識別碼

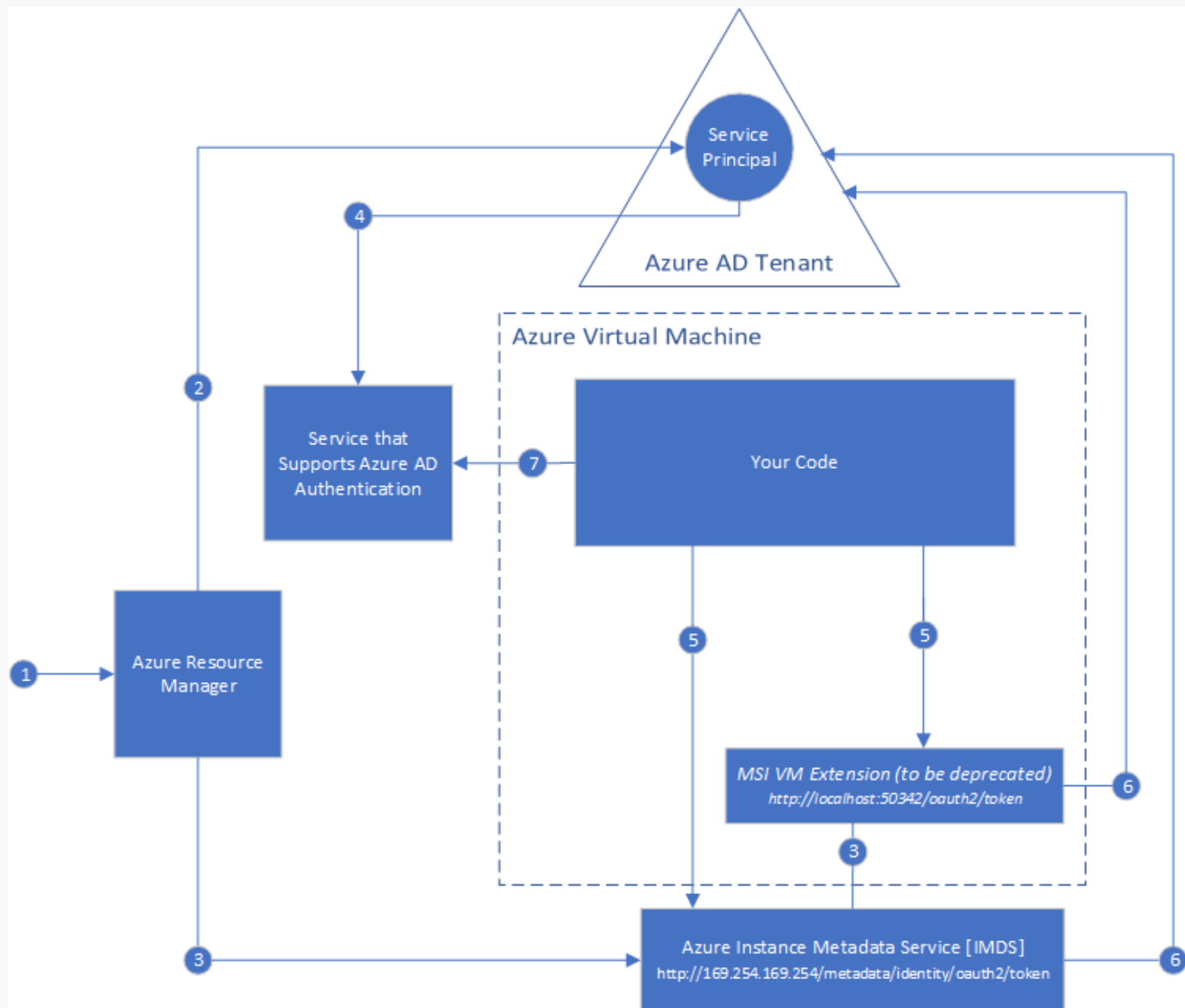
- 控制之服務主體的識別碼，可用來將角色型存取授與 Azure 資源

- Azure Instance Metadata Service (IMDS)

- REST 端點，可讓 Azure VM 來存取，可透過 (169.254.169.254) 取得資訊，該位址只能從 VM 內存取。

架構與原理

1. 收到啟用 VM 受控識別請求
2. 在 AAD 建立 SP
(代表 VM / 自行建立的 SP)
3. 將 ClientID 和憑證更新 IMDS，
並在 VM 上註冊身分
4. 將 VM 授予 Azure 資源存取權
EX : Key Vault
5. 程式碼要存取時，透過 IMDS
要求授權
可對 MSI 外掛 / IMDS 提出要求
6. 將 ClientID 和憑證傳回 AAD
並取得 JWT
7. 透過 JWT 控制 Azure 資源



兩種模式

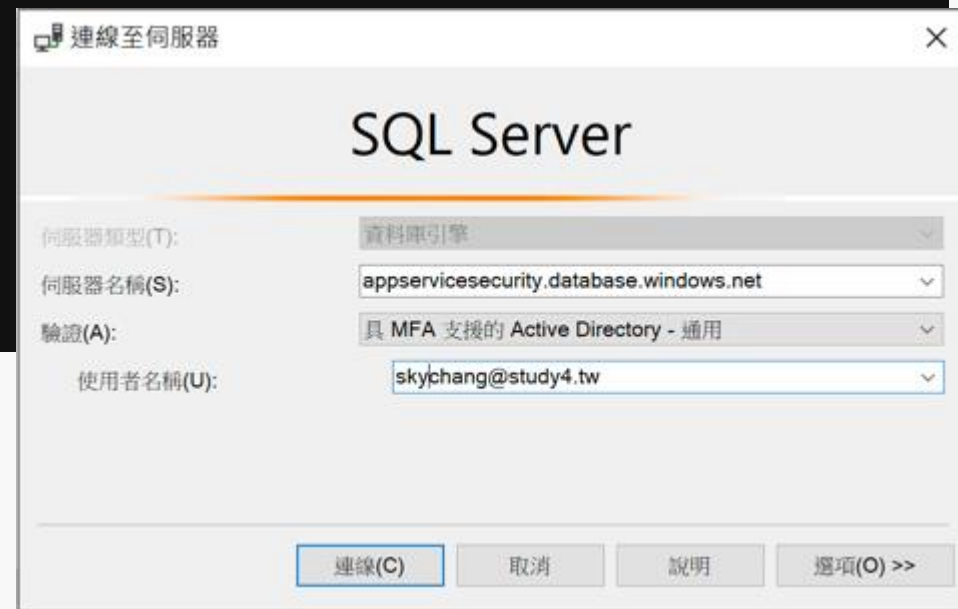
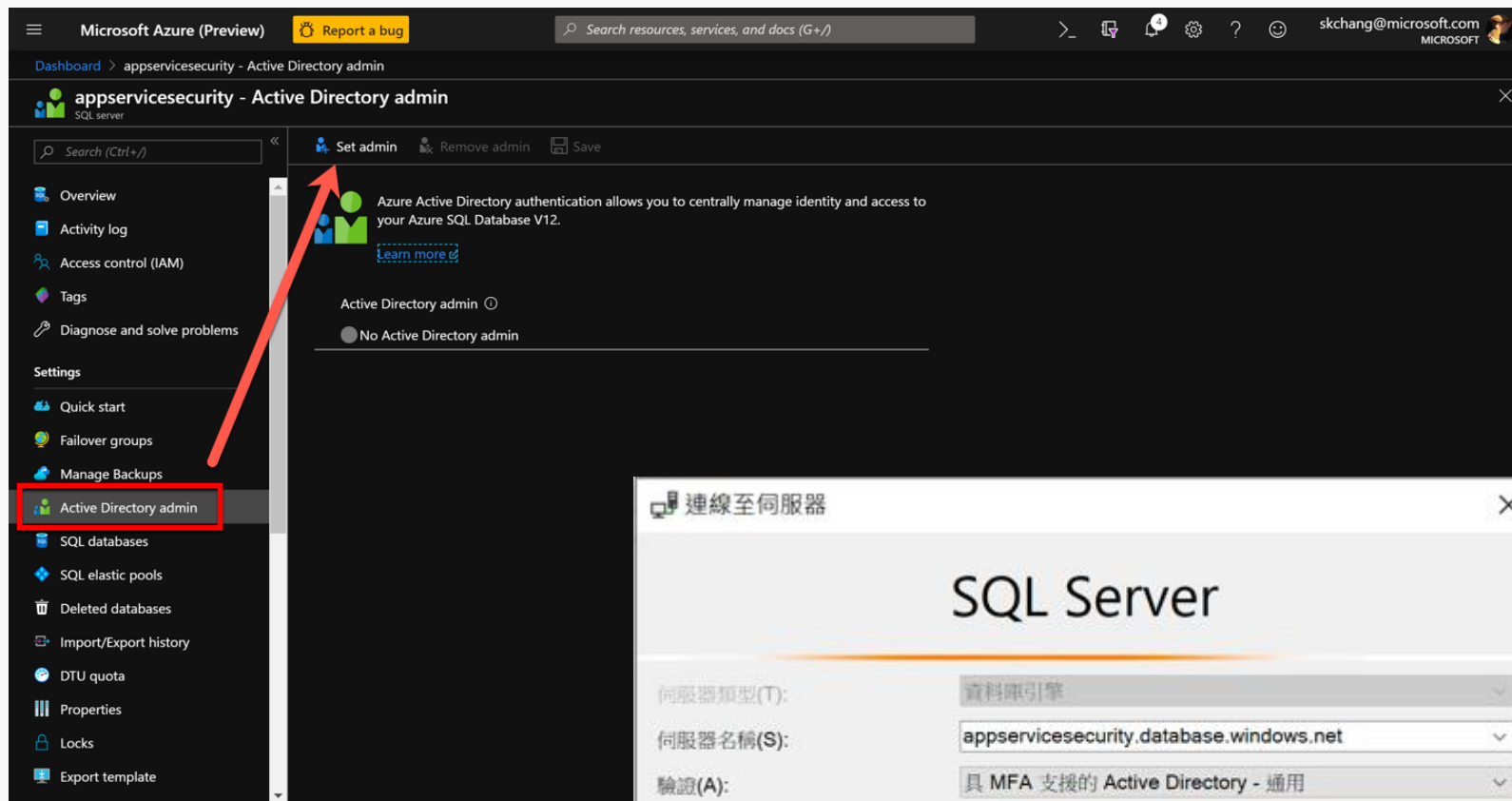
	系統指派的受控識別	使用者指派的受控識別
建立	為 Azure 資源的一部分 (例如 Azure VM 或 Azure App Service)	為獨立的 Azure 資源
生命週期	與 Azure 資源共用生命週期。 當父代資源刪除時，受控識別也會一併刪除。	獨立的生命週期。 必須明確刪除。
由其他 Azure 資源共用	無法共用。 它只能與單一 Azure 資源關聯。	可以共用 使用者可指派同一個受控識別可與多個 Azure 資源相關聯。
一般使用案例	單一 Azure 資源內的工作負載 當串接其他工作需要進行識別時 ex：在 VM 上執行的應用程式、App Service 等	在多個資源上執行、使用同一個身分識別 在自動化建置流程中需要預先授權以保護資源的工作 資源回收頻率高、但權限應保持一致的工作 ex：有多個 VM 需要存取相同資源的工作

Demo App Service + Managed identities for Azure resources



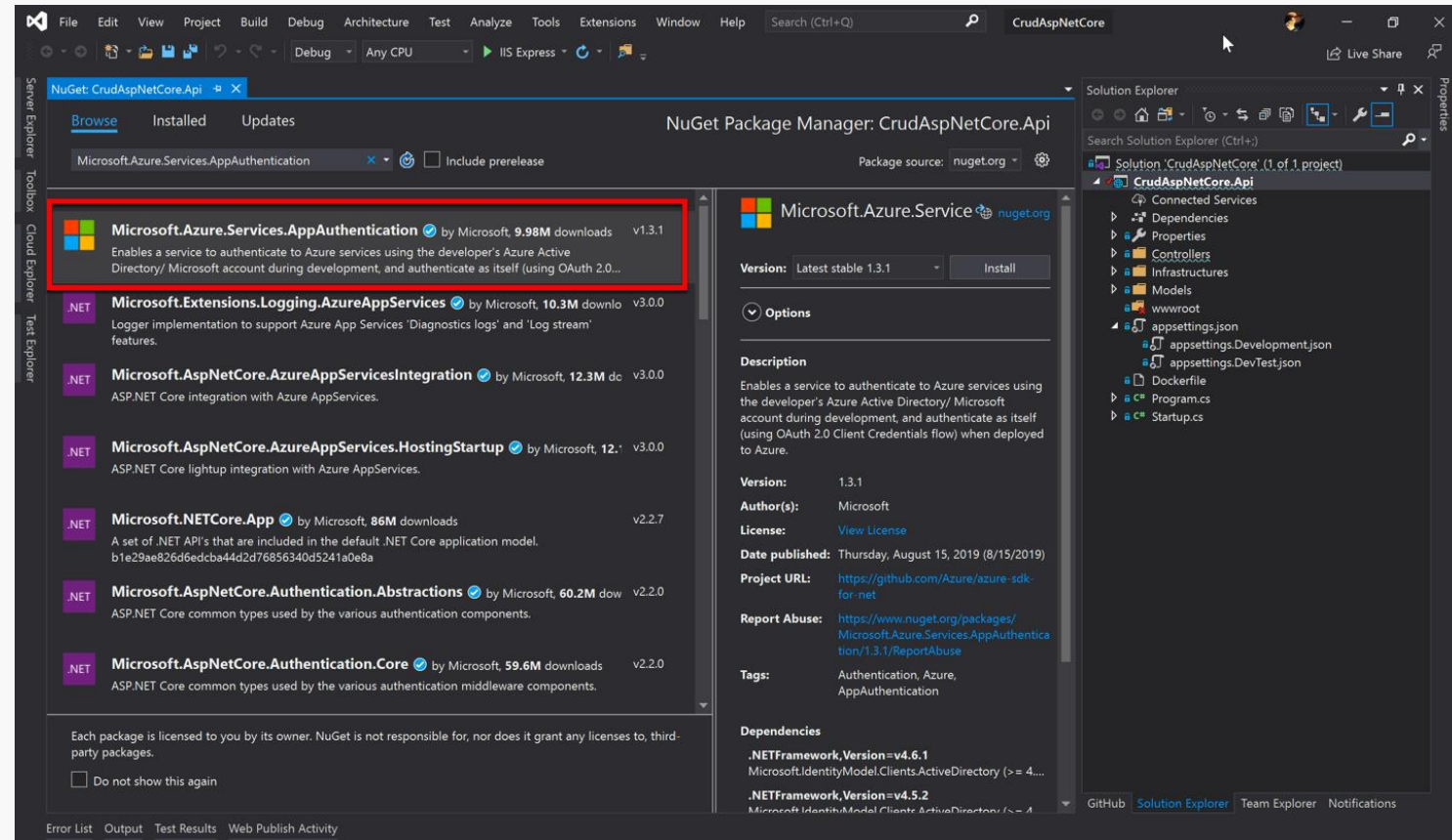
使用 AAD 帳號當 SQL Database 的系統管理員

- 使用現有 AAD 帳號登入
- 可以透過 SSMS 登入
- 防火牆別忘記開
- 整個流程非必要，但可以強化 DB 管理
- 若是測試資料庫也很方便開發



Microsoft.Azure.Services.AppAuthentication

- 程式需要小修改，來取得 Token
- AzureServiceTokenProvider 類別會快取記憶體中的權杖



ASP.NET Core 的調整

- 在建構子取回 Connection 物件，並加上 取回的 Token
- 連線字串可以不需要存取帳密
- 不支援 Initial Catalog 字串

```
namespace CrudAspNetCore.Api.Infrastructure
{
    5 references | 0 changes | 0 authors, 0 changes
    public class SkyHRContext : DbContext
    {
        0 references | 0 changes | 0 authors, 0 changes
        public SkyHRContext(DbContextOptions<SkyHRContext> options)
            : base(options)
        {
            var conn = (SqlConnection)Database.GetDbConnection();
            conn.AccessToken = (new AzureServiceTokenProvider())
                .GetAccessTokenAsync("https://database.windows.net/").Result;
            Database.EnsureCreated();
        }
    }
}
```

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Debug",
      "System": "Information",
      "Microsoft": "Information"
    }
  },
  "ConnectionStrings": {
    "DefaultConnection": ""
  }
}
```

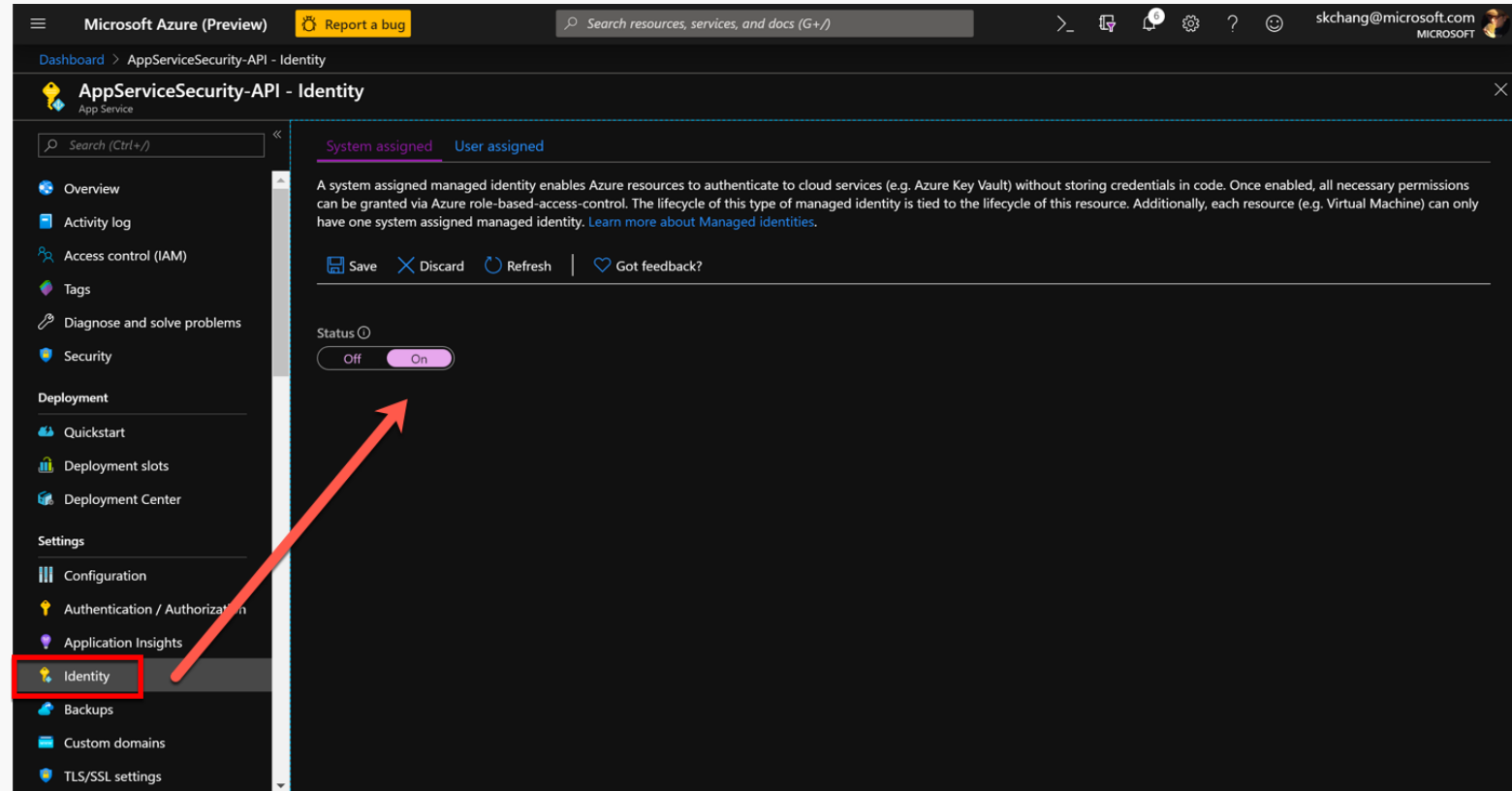
ASP.NET Core 的調整 II

- 不要使用 AddDbContextPool，會發生 login 失敗，需要每次都重建 DbContext

```
// 注意，除了不同環境有不同的 appsetting 外，目前還有可能使用到 Secret Management  
// 目前使用 AddDbContextPool 會發生 login 失敗  
services.AddDbContext<SkyHRContext>(options =>  
    options.UseSqlServer(Configuration.GetConnectionString("DefaultConnection")));
```

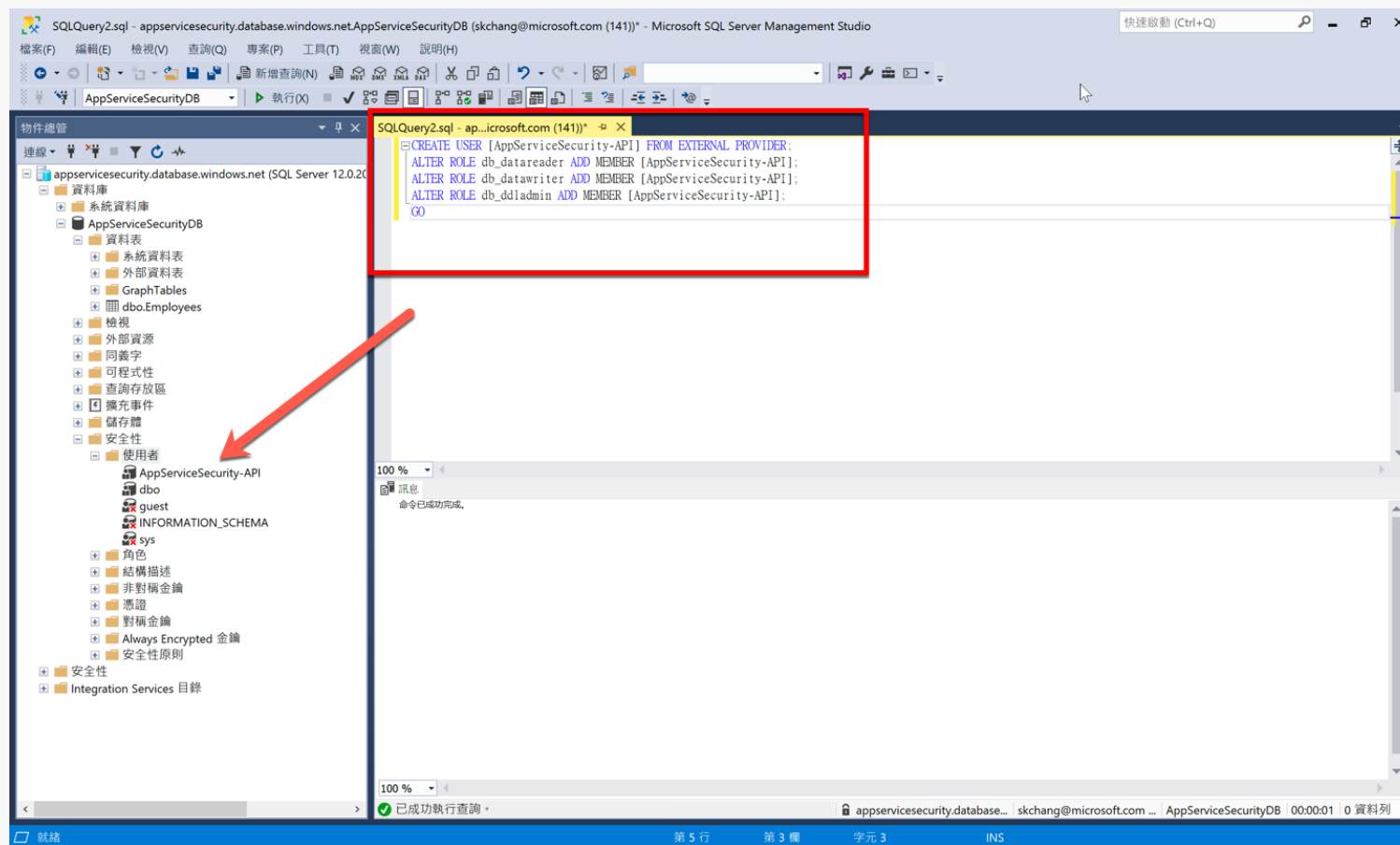
App Service 設定

- App Service 開啟 Identity
- 會去 AAD 註冊 App Service
- 名稱和此 App Service 同



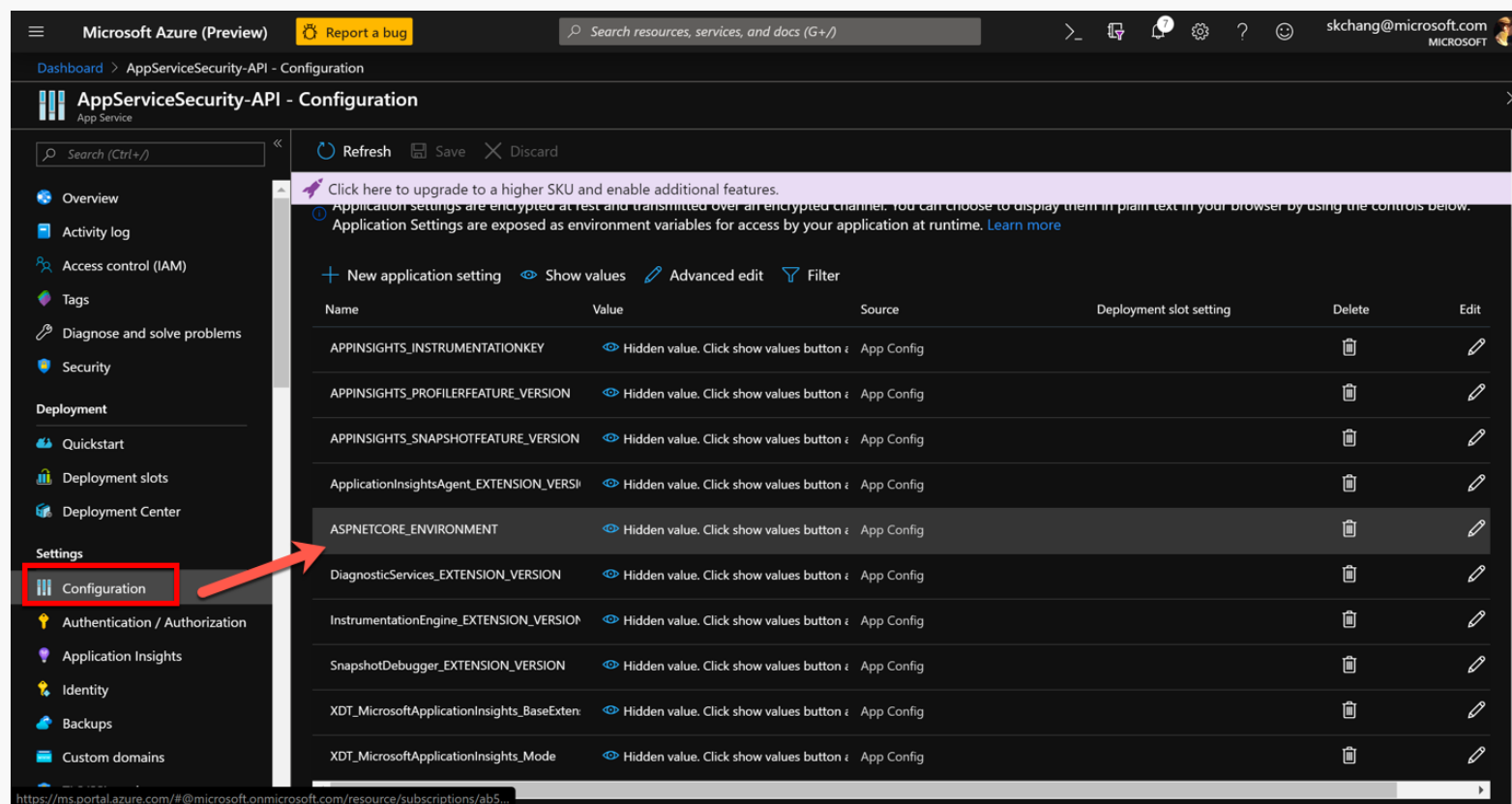
SQL Database 加入新的使用者

- 透過 SSMS 新增 User
- User 名稱為 Web App Service 名稱



注意環境變數

- 發佈上去後，不用設定連線字串
- 但要注意 ASP.NET Core 的環境



問題..

- 雖然連線字串的帳密改成 MSI，但上面還是有 SQL Database 位置阿!!
 - 可不可以連“連線字串”都消失不見?

Azure Key Vault



Azure Key Vault

- **祕密管理**

- 可用來安全地儲存權杖、密碼、憑證、API 金鑰和其他機密，並嚴密控制其存取

- **金鑰管理**

- 可作為金鑰管理解決方案

- **憑證管理**

- 輕鬆地佈建、管理及部署 Azure 和您內部連線的資源所使用的公用和私人安全通訊端層/傳輸層安全性 (SSL/TLS) 憑證

- **儲存受到硬體安全性模型支援的機密**

- 機密和金鑰可受到軟體的保護，或由通過 FIPS 140-2 Level 2 驗證的 HSM 保護

Azure Key Vault

- 集中儲存應用程式祕密

- 不需要在每一個應用程式 (或是 Service) 儲存資訊

- 安全地儲存秘密和金鑰

- 使用標準演算法、高長度的金鑰、硬體安全性模組 (HSM) 來保護機密和金鑰
- HSM 經過美國聯邦資訊處理標準 (FIPS) 140-2 Level 2 驗證
- 存取需要經過驗證與授權 (AAD)
- Microsoft 也無法看到其內容

- 監視存取和使用

- 可串流到 Storage、Event Hub、Azure Monitor

Azure Key Vault

- 簡化應用程式的管理

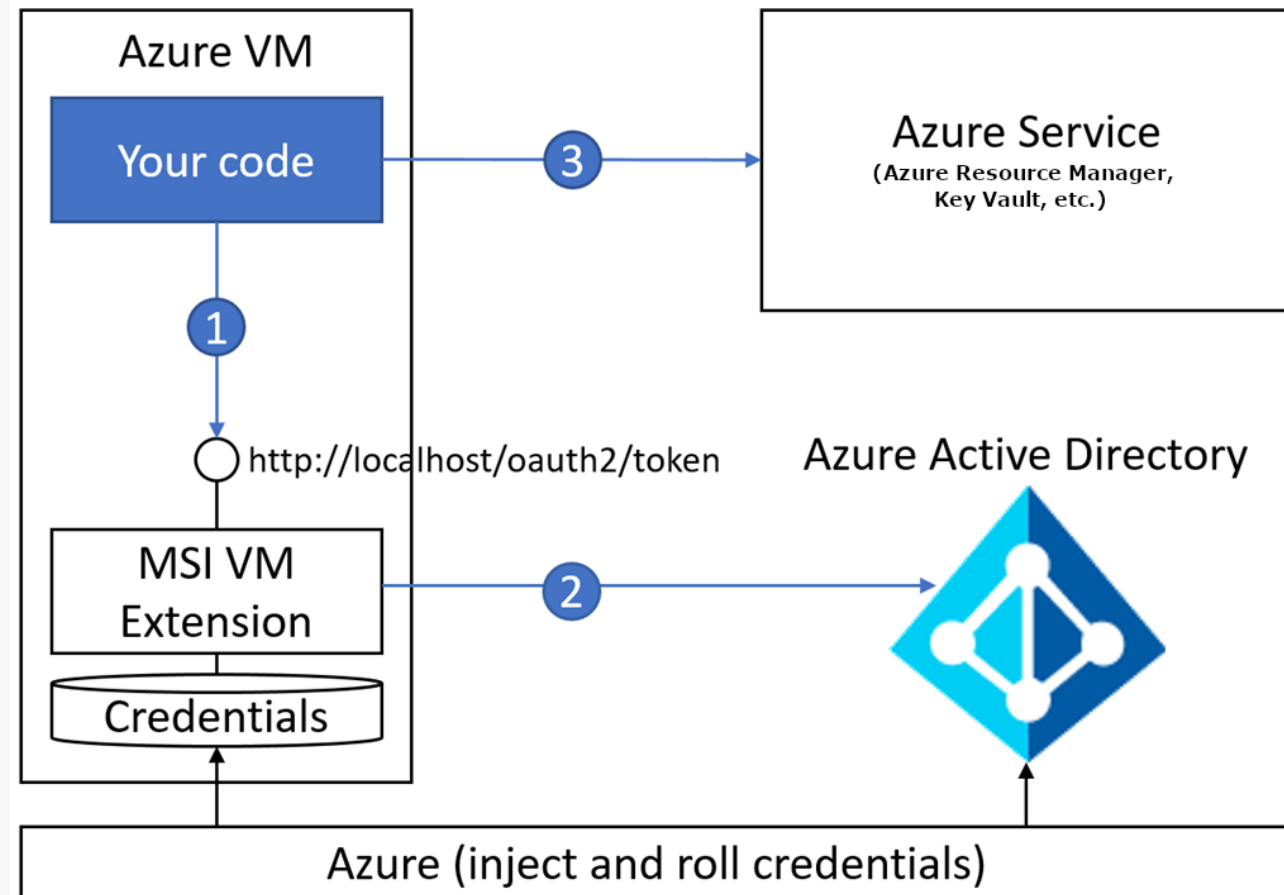
- 不需要知道硬體安全性模組知識，立刻可以使用!
- 提供 Scale Out !!，提供組織尖峰使用
- 將 Key Vault 內容複寫到其他區域，自動處理 HA & DR
- 管理方便，透過入口網站、Azure CLI 或 PowerShell 進行管理
- 自動對公開 CA 購買的憑證，簡化註冊或續約作業
- 輕鬆隔離每個應用程式，應用程式只能存取自己的保存庫
- 可為每個應用程式建立 Azure Key Vault，並將 Key Vault 限制於特定應用程式和開發人員

- 和 Azure Service 整合密切

- Azure 磁碟的加密
- SQL Server、Azure SQL Database 的 Always Encrypted
- Azure App Service

Your Code + Key Vault

1. 程式透過端點和 AAD 取得 Token
(雖然用 Key Vault 隱藏資訊，但驗證授權還是需要透過 MSI)
2. AAD 返回 Token
3. 程式使用 Token 和 Key Vault 要資料



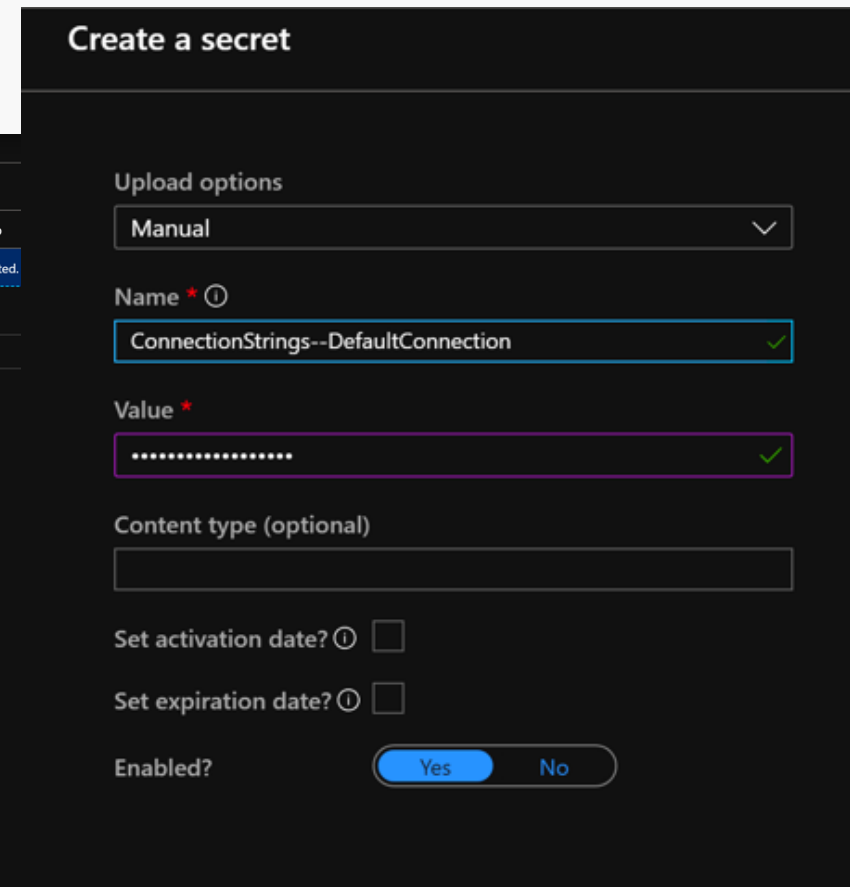
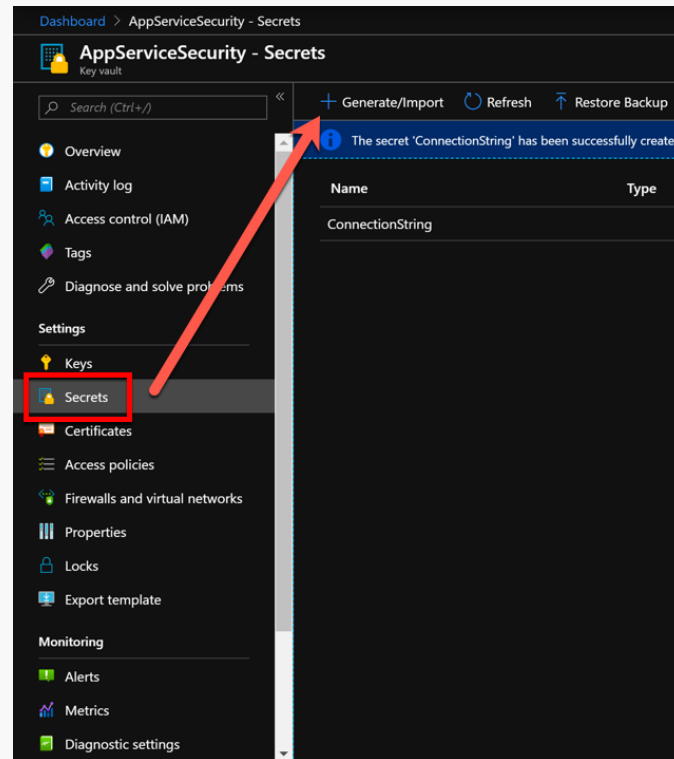
Demo App Service + Azure Key Vault Part I



將連線字串寫入 Azure Key Vault

在 ASP.NET Core CLI Secret Management 使用：當作階層
在 Key Vault 裡面使用 -- 當作階層

Ex : appsettings.json 的 Connection String
要使用 ConnectionStrings--DefaultConnection



授予 Azure Key Vault 權限

- 設定權限
- 主要為 get list
- 使用者為 App Service

Microsoft Azure (Preview) Report a bug

Dashboard > AppServiceSecurity - Access policies

AppServiceSecurity - Access policies

Search (Ctrl+J)

Save Discard Refresh

Please click 'Save' button to commit your changes

Enable Access to:

- ☐ Azure Virtual Machines for deployment
- ☐ Azure Resource Manager for template deployment
- ☐ Azure Disk Encryption for volume encryption

+ Add Access Policy

Current Access Policies

Name	Category
APPLICATION	
AppServiceSecurity-API	APPLICATION
USER	
Sky Chang	USER

Sky.Chang@microsoft... 9 selected 7 selected 15 selected Delete

Configure from template (optional)

Key permissions: 0 selected

Secret permissions: 2 selected

Certificate permissions: 0 selected

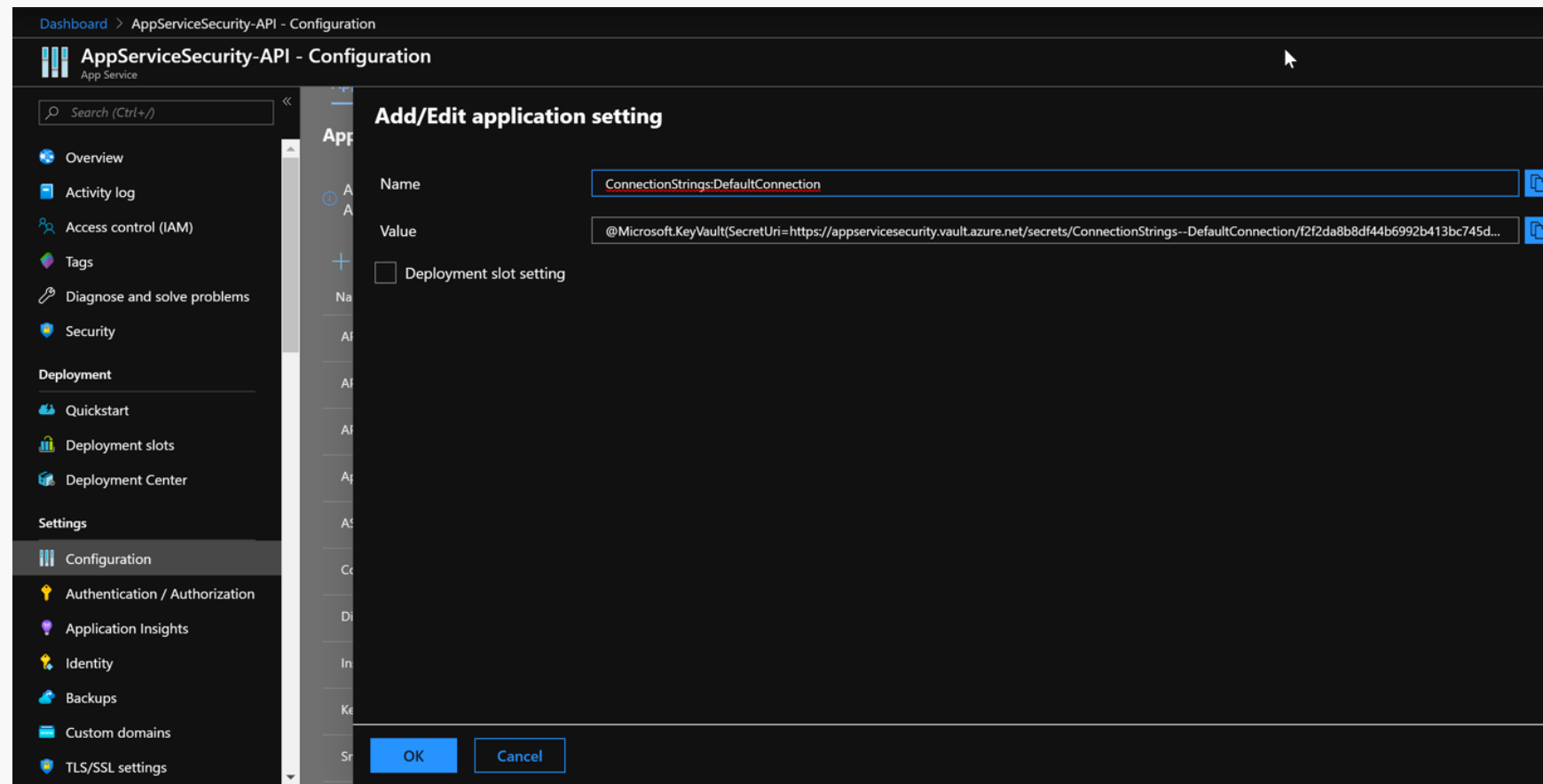
Select principal: AppServiceSecurity-API

Authorized application: None selected

直接設定 AppService Config

- @Microsoft.KeyVault(SecretUri=https://appservicesecurity.vault.azure.net/secrets/ConnectionStrings--DefaultConnection/f2f2da8b8df44b6992b413bc745d10d0)

- 使用快速
- 不需要動用到程式碼



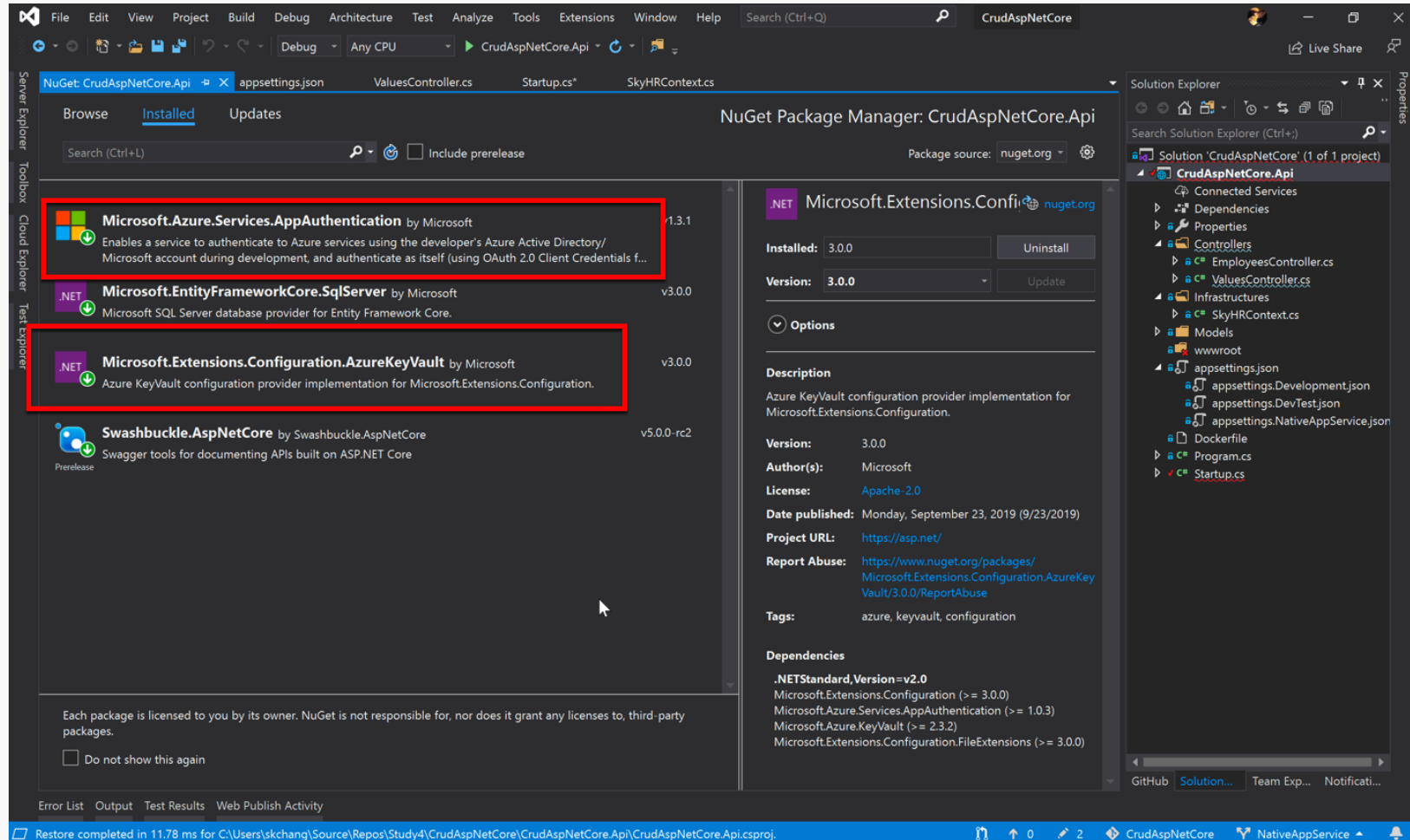
Demo App Service + Azure Key Vault Part II



安裝 NuGet Package












Microsoft.Azure.Services.AppAuthentication
Microsoft.Extensions.Configuration.AzureKeyVault

AppAuthentication 處理驗證
AzureKeyVault 處理機密字串



App Service 設定

- 不需要設定 `ConnectionString`
- 若有需要，只需要提供 `KeyVault` 網址
- Linux 請使用 `_`
- Windows 可以使用 `_` 或是：

Name	Value	Source	Deploy
APPINSIGHTS_INSTRUMENTATIONKEY	 Hidden value. Click show values button >	App Config	
APPINSIGHTS_PROFILERFEATURE_VERSION	 Hidden value. Click show values button >	App Config	
APPINSIGHTS_SNAPSHOTFEATURE_VERSION	 Hidden value. Click show values button >	App Config	
ApplicationInsightsAgent_EXTENSION_VERSION	 Hidden value. Click show values button >	App Config	
ASPNETCORE_ENVIRONMENT	 Hidden value. Click show values button >	App Config	
DiagnosticServices_EXTENSION_VERSION	 Hidden value. Click show values button >	App Config	
InstrumentationEngine_EXTENSION_VERSION	 Hidden value. Click show values button >	App Config	
KeyVault_BaseUrl	 Hidden value. Click show values button >	App Config	
SnapshotDebugger_EXTENSION_VERSION	 Hidden value. Click show values button >	App Config	
XDT_MicrosoftApplicationInsights_BaseExtension	 Hidden value. Click show values button >	App Config	
XDT_MicrosoftApplicationInsights_Mode	 Hidden value. Click show values button >	App Config	

ASP.NET Core 3 設定

開發環境連線字串吃 Secret Management

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Debug",
      "System": "Information",
      "Microsoft": "Information"
    }
  },
  "ConnectionStrings": {
    "DefaultConnection": ""
  }
}
```

appsettings.Development.json

Name	Value	Source	Deploy
APPINSIGHTS_INSTRUMENTATIONKEY	Hidden value. Click show values button	App Config	
APPINSIGHTS_PROFILERFEATURE_VERSION	Hidden value. Click show values button	App Config	
APPINSIGHTS_SNAPSHOTFEATURE_VERSION	Hidden value. Click show values button	App Config	
ApplicationInsightsAgent_EXTENSION_VERSION	Hidden value. Click show values button	App Config	
ASPNETCORE_ENVIRONMENT	Hidden value. Click show values button	App Config	
DiagnosticServices_EXTENSION_VERSION	Hidden value. Click show values button	App Config	
InstrumentationEngine_EXTENSION_VERSION	Hidden value. Click show values button	App Config	
KeyVault_BaseUrl	Hidden value. Click show values button	App Config	
SnapshotDebugger_EXTENSION_VERSION	Hidden value. Click show values button	App Config	
XDT_MicrosoftApplicationInsights_BaseExtension	Hidden value. Click show values button	App Config	
XDT_MicrosoftApplicationInsights_Mode	Hidden value. Click show values button	App Config	

NativeAppService

<https://appservicesecurity.vault.azure.net/>

App Service

環境為 NativeAppService 啟動

```
1 reference | Sky Chang, 187 days ago | 1 author, 1 change
public static IHostBuilder CreateHostBuilder(string[] args) =>
    Host.CreateDefaultBuilder(args)
        .ConfigureAppConfiguration((context, config) =>
        {
            if (context.HostingEnvironment.EnvironmentName == "NativeAppService")
            {
                var builtConfig = config.Build();
                var azureServiceTokenProvider = new AzureServiceTokenProvider();
                var keyVaultClient = new KeyVaultClient(
                    new KeyVaultClient.AuthenticationCallback(
                        azureServiceTokenProvider.KeyVaultTokenCallback));
                config.AddAzureKeyVault(
                    builtConfig["KeyVault:BaseUrl"],
                    keyVaultClient,
                    new DefaultKeyVaultSecretManager());
            }
        })
        .ConfigureWebHostDefaults(webBuilder =>
        {
            webBuilder.UseStartup<Startup>();
        });
```

將 Key Vault map 到設定

Program.cs

```
{
  "ConnectionStrings": {
    "DefaultConnection": "Server=(localdb)\\mssqllocaldb;Database=SkyHRDB;Trusted_Connection=true;TrustServerCertificate=true;"
  }
}
```

Secret Management

吃 Config 的順序

Local

App Service

判斷環境變數

Secret Management

Azure Key Vault

App Service Config

appsettings.json

Microsoft.Azure.KeyVault

- 如果只是單純的想取得 Value 可以用底下的 Code
- 需安裝 Microsoft.Azure.KeyVault

```
try
{
    AzureServiceTokenProvider azureServiceTokenProvider
        = new AzureServiceTokenProvider();
    KeyVaultClient keyVaultClient = new KeyVaultClient(
        new KeyVaultClient.AuthenticationCallback(azureServiceTokenProvider.KeyVaultTokenCallback));
    var secret = await keyVaultClient
        .GetSecretAsync("https://<YourKeyVaultName>.vault.azure.net/secrets/AppSecret").ConfigureAwait(false);
    var Message = secret.Value;
}
catch (KeyVaultErrorException keyVaultException)
{
}
}
```

問題..

- 我的 API 不想對外...
 - 可不可以讓 Internet 無法存取我的 API

Service Endpoints

Service Endpoints

- 改善 Azure 服務資源的安全性
 - 建立規則!移除 Azure 資源上的公用網路存取
 - 可只允許來自虛擬網路的流量
- 使用虛擬網路最佳路由來處理 Azure 服務
 - 預設 Azure Service 會透過 Internet 路由到你的虛擬設備 (forced-tunneling)
 - Service Endpoints 不走預設路線，直接使用 Azure 骨幹網路
- 設定簡單且管理負擔小
 - 服務不需要公用 IP，也不需要再設定對外的防火牆
 - 不需要 NAT / Gateway 設備來設定
- 免費、免費、免費

限制

- 僅限 Azure Resource Manager 部署的 VNET
- 內部資源無法使用
- Azure SQL 只限定於 VNET 所在區域

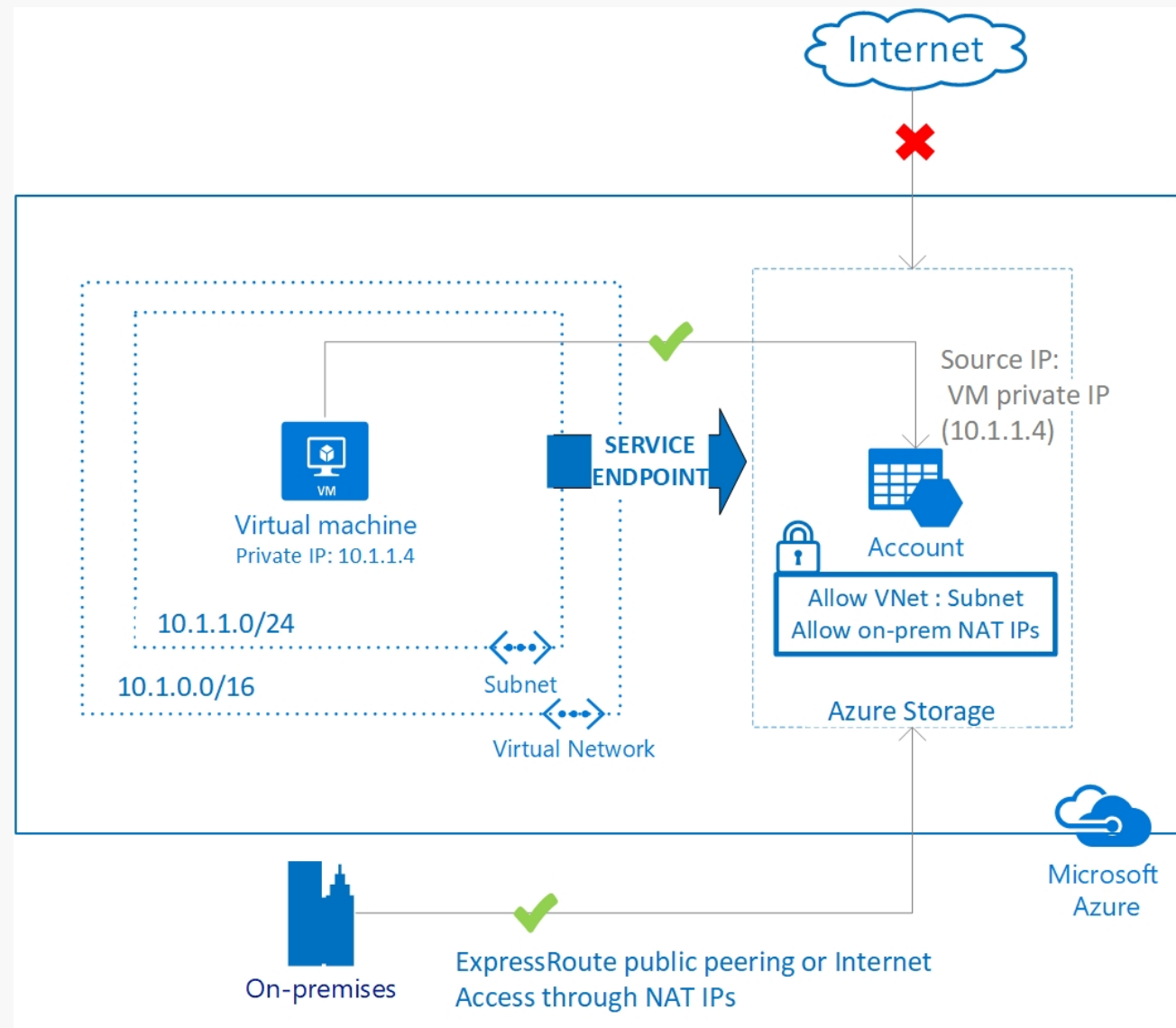
支援服務 2018/8/5

- GA -
- Azure Storage
- Azure SQL Database
- Azure SQL Data Warehouse
- Azure Database for PostgreSQL server
- Azure Database for MySQL server
- Azure Database for MariaDB
- Azure Cosmos DB

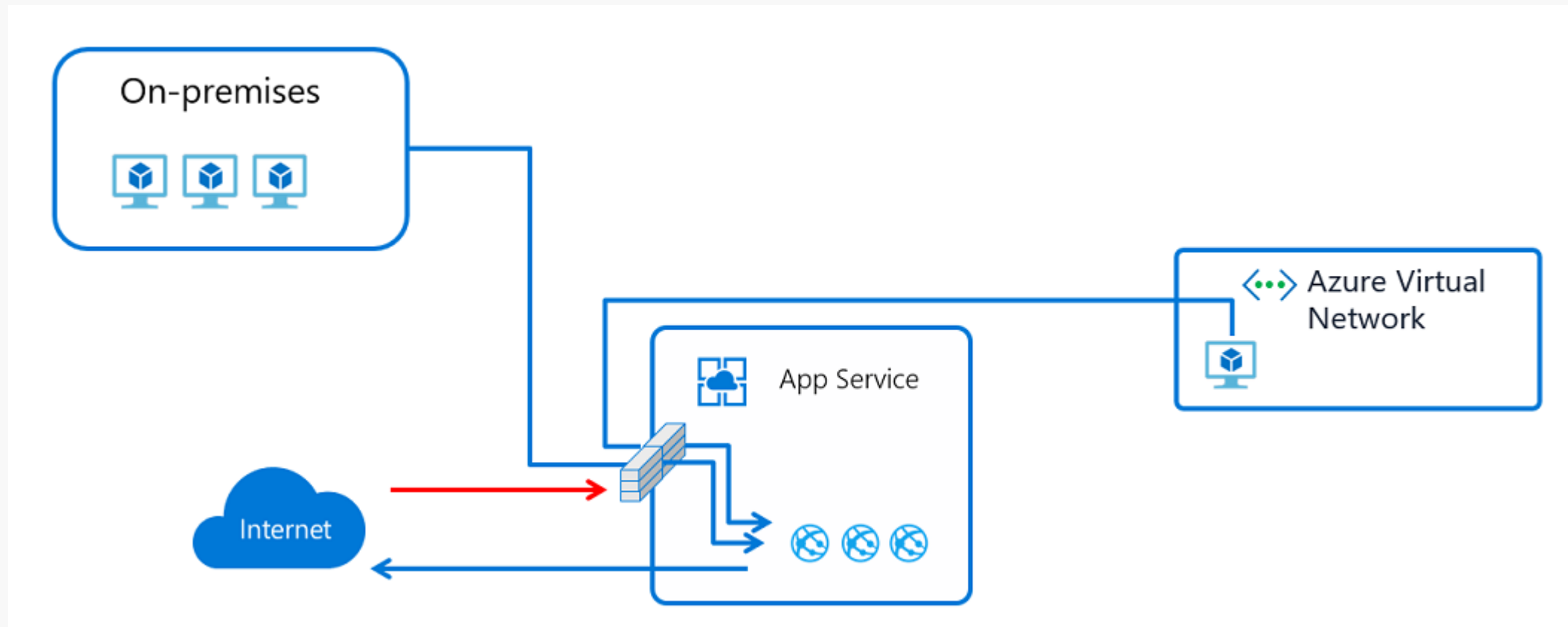
- GA -
- Azure Key Vault
- Azure Service Bus
- Azure Event Hubs
- Azure Data Lake Store Gen 1
- Azure App Service
- 預覽階段 -
- Azure Container Registry

架構

- Storage 的 URL (對外 IP 還是固定) 透過 Service Endpoint 會自動轉換 (防火牆不需要調整)
- 內部不能使用 Service Endpoint, 必須透過 ExpressRoute 保護安全



App Service and Service Endpoints

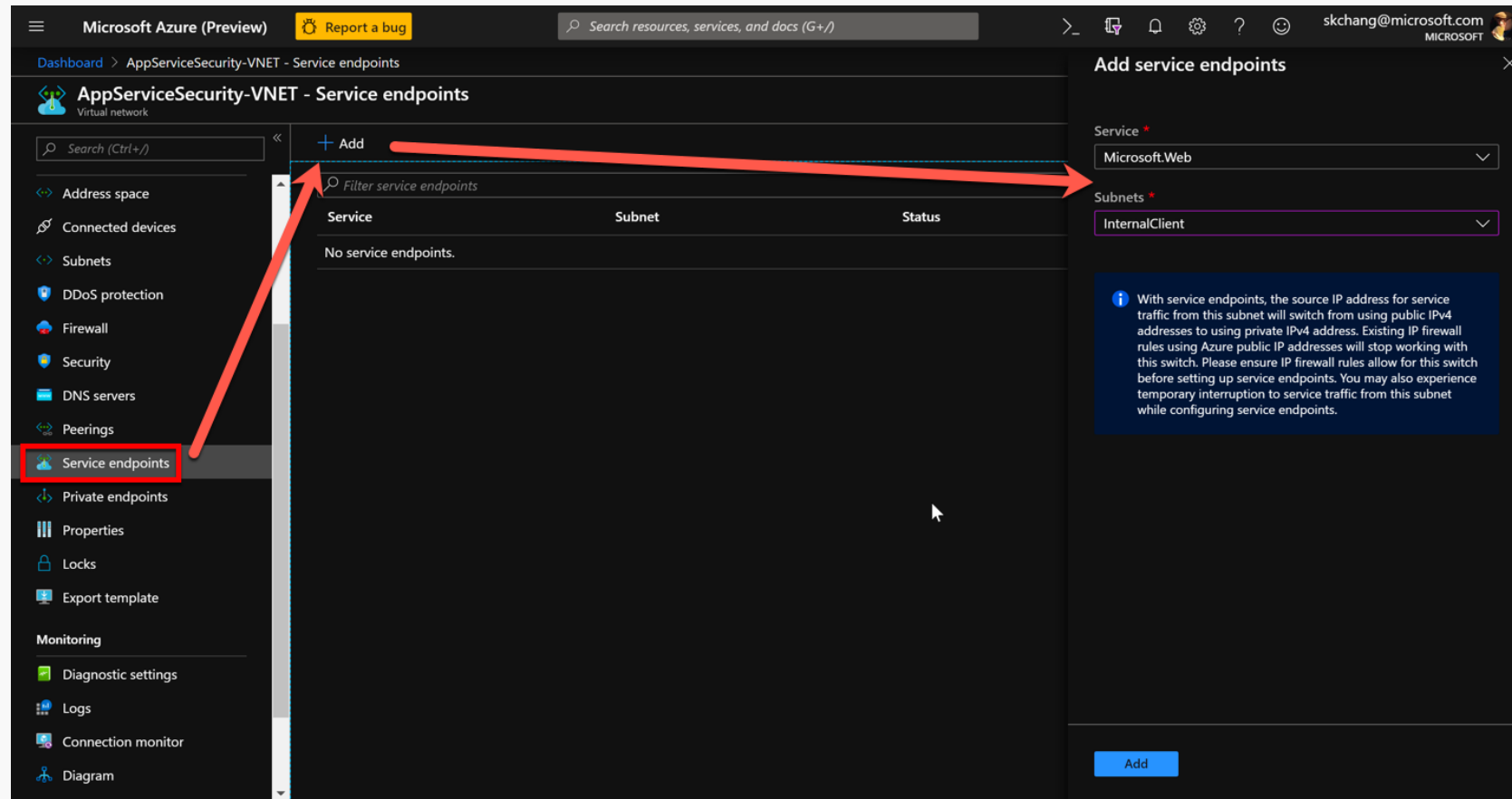


Demo App Service + Service Endpoints



啟用 VNET Service Endpoints

- 請注意，連線可能會中斷
- 也不一定要先啟用



設定 App Service

Dashboard > AppServiceSecurity-API - Networking

AppServiceSecurity-API - Networking

App Service

Search (Ctrl+/)

- Authentication / Authorization
- Application Insights
- Identity
- Backups
- Custom domains
- TLS/SSL settings
- Networking**
- Scale up (App Service plan)
- Scale out (App Service plan)
- WebJobs
- Push
- MySQL In App
- Properties
- Locks
- Export template
- App Service plan
 - App Service plan
 - Quotas

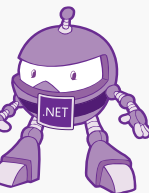
Securely access resources available in or through your Azure VNet.
[Learn More](#)
[Click here to configure](#)

Hybrid connections
Securely access applications in private networks
[Learn More](#)
[Configure your hybrid connection endpoints](#)

Azure Front Door with Web Application Firewall
Scalable and secure entry point for accelerated delivery of your web applications
[Learn More](#)
[Configure Azure Front Door with WAF for your app](#)

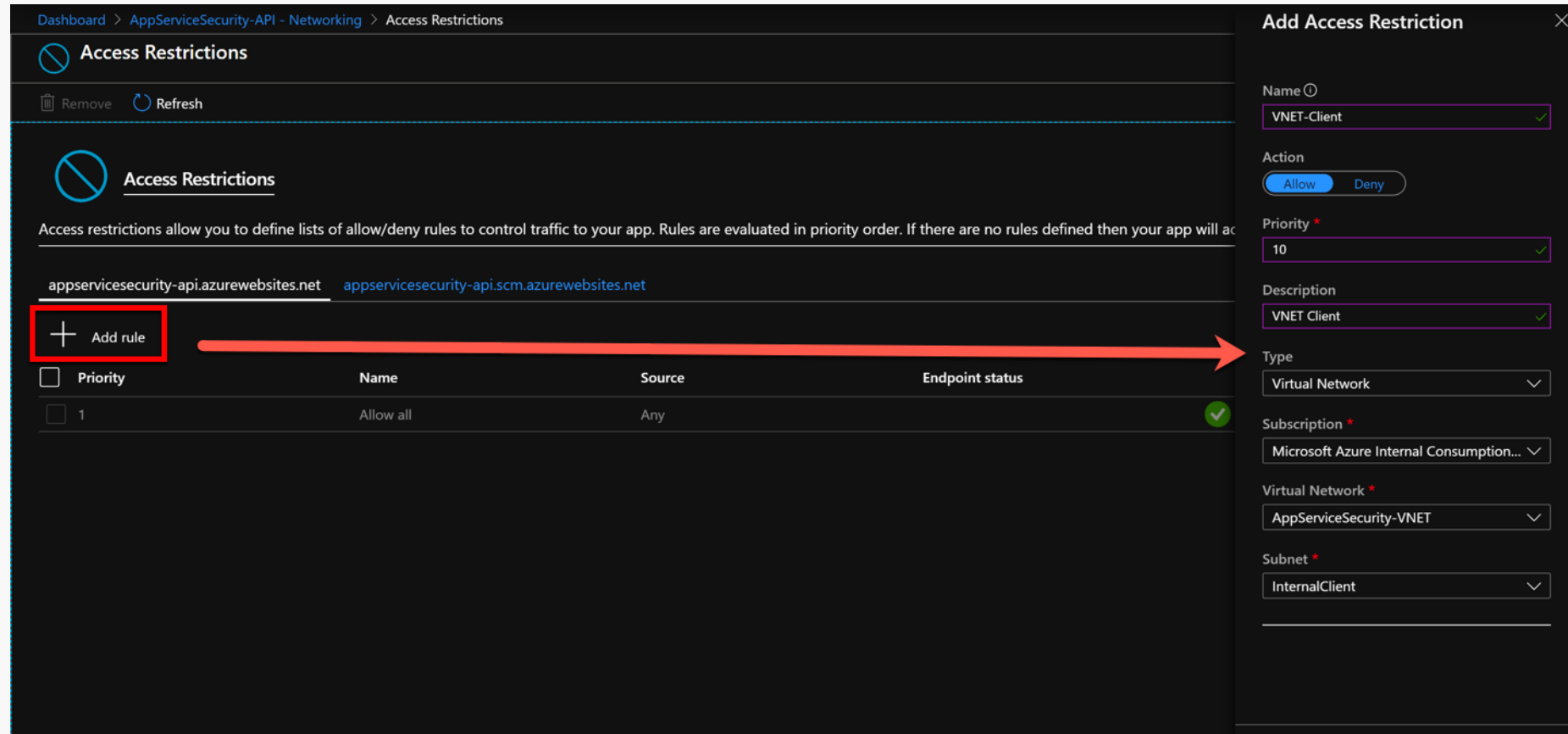
Azure CDN
Secure, reliable content delivery with broad global reach and rich feature set
[Learn More](#)
[Configure Azure CDN for your app](#)

Access Restrictions
Define and manage rules that control access to your application.
[Learn More](#)
[Configure Access Restrictions](#)



選擇使用 Service Endpoints

- 選擇使用 Service Endpoints
- 設定完後，外部 IP 就無法存取，僅限 Azure 內部使用



Dashboard > AppServiceSecurity-API - Networking > Access Restrictions

Access Restrictions

Remove Refresh

Access restrictions allow you to define lists of allow/deny rules to control traffic to your app. Rules are evaluated in priority order. If there are no rules defined then your app will accept all traffic.

appservicesecurity-api.azurewebsites.net appservicesecurity-api.scm.azurewebsites.net

+ Add rule

Priority	Name	Source	Endpoint status
1	Allow all	Any	✓

Add Access Restriction

Name ○ VNET-Client ✓

Action Allow Deny

Priority * 10 ✓

Description VNET Client ✓

Type Virtual Network ✓

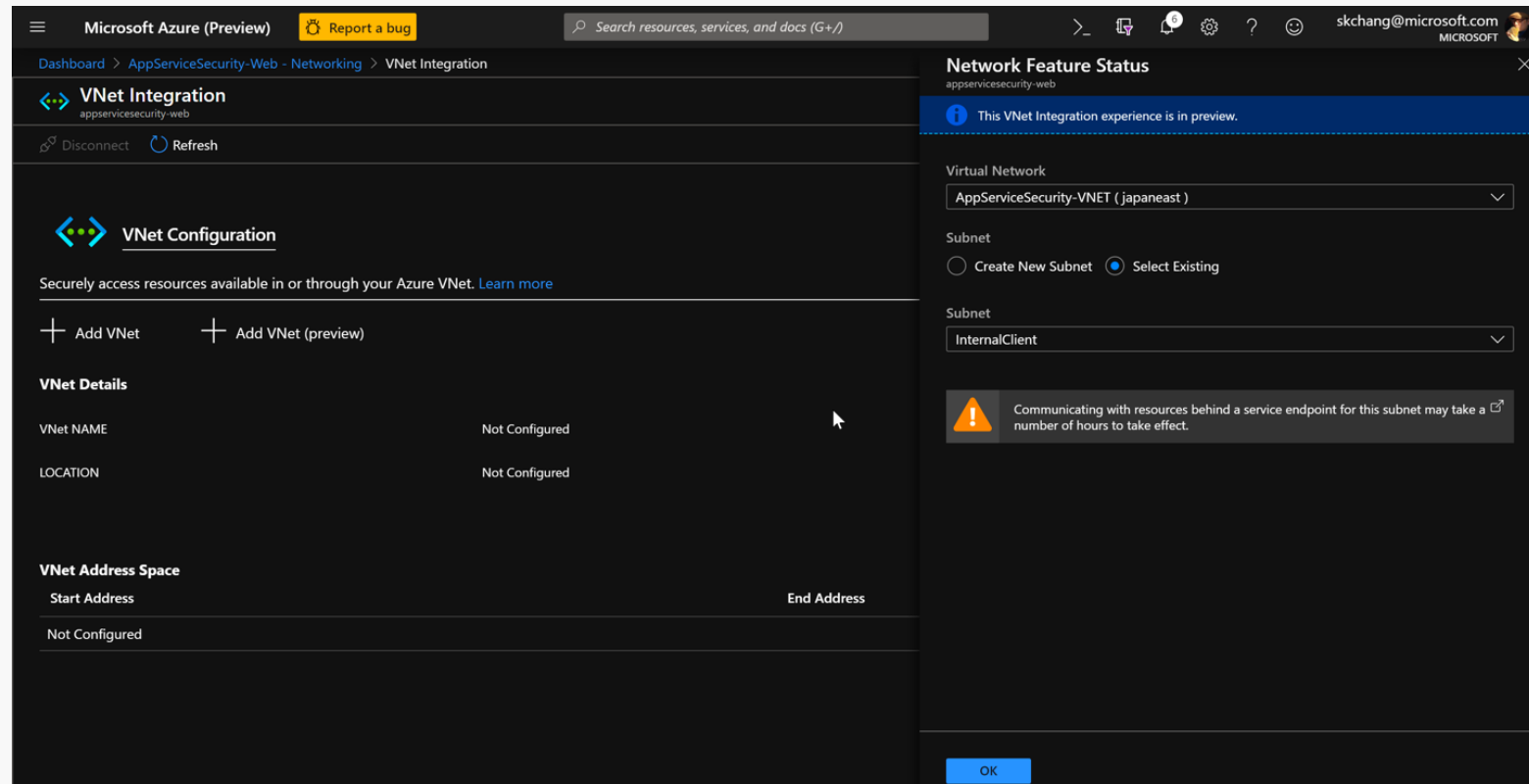
Subscription * Microsoft Azure Internal Consumption... ✓

Virtual Network * AppServiceSecurity-VNET ✓

Subnet * InternalClient ✓

設定前端頁面

- 請注意，若有前端頁面，這個頁面必須在 VNET 裡面才能存取後端
- 若不同 Subnet，要記得全部重做
- 設定完可能要等 10 min 生效



App Service 回顧

App Service Security

- 隨時保持更新
 - 應用程式更新、系統自動更新
- 身分識別與存取管理
 - 停用匿名、啟用身分認證
 - 使用驗證存取後端 (使用憑證) - MSI
- 資料保護
 - 啟用 Https (重新導向) – 透過 ASP.NET Core
 - 不放置敏感資訊 – Key Vault
- 網路相關
 - 限制 IP – Service Endpoints
- 監視
 - Log 紀錄，安全中心 – ApplicationInsight

.NET Conf

探索 .NET 新世界

THANK YOU

Host by
STUDY4

