

Jeśli aplikacja ma być skalowalna i odporna na awarie poszczególnych serwerów to będzie potrzebny Load Balancer.

Load balancer przyjmuje rządania z zewnątrz (od klientów) a następnie te rządania dystrybuuje do serwerów, które wykonują określone czynności. Load balancer z jednej strony obsługuje jeden adres IP a z drugiej wiele adresów poszczególnych serwerów. Istnieją różne polityki rozdzielania zadań: losowa, próba wysyłania takich samych ilości do wszystkich, wysyłanie na podstawie prędkości odpowiedzi serwera.

Dla aplikacji webowych powstał specjalny load balancer – Azure Application Gateway, który dba o to aby raz nawiązane połączenie trafiało do tego samego serwera po stronie aplikacji. Inna funkcja AAG to wyświetlanie informacji o błędzie jeśli klient rządu wyświetlenia nieistniejącej strony.

Inna funkcja to rozpakowywanie pakietów SSL żeby serwery odpowiadające za generowanie strony nie poświęcały swojej mocy obliczeniowej na szyfrowanie danych.

W Azure Application Gateway można skonfigurować Azure Web Application Firewall, który może identyfikować próby włamania.

Azure Application Gateway to coś innego niż Azure VPN Gateway. VPN pozwala na ustanowienie połączenia z Azure do on premises czyli do robienia chmury hybrydowej.

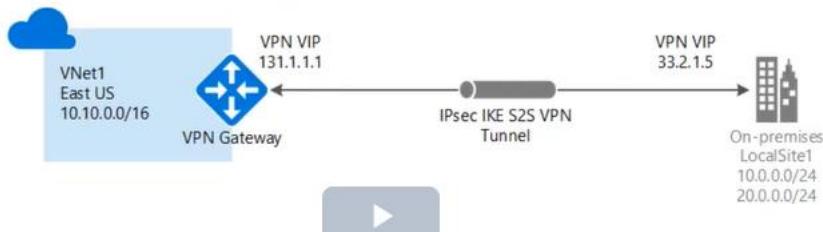
Ogólnie rzecz ujmując Azure VPN Gateway odpowiada na to aby urządzenia znajdujące się na zewnątrz sieci wirtualnej były w stanie do tej sieci się podłączyć. Dzieje się to przez stworzenie dedykowanego tunelu. Istnieją 3 różne sposoby połączenia do VPN Gateway:

1. Site to site S2S – sieć wirtualna jest połączona z jedną lokalizacją po stronie on premises. Po stronie Azure jest VPN Gateway a po stronie on premises urządzenie z publicznym adresem IP.

### Site-to-Site and Multi-Site (IPsec/IKE VPN tunnel)

#### Site-to-Site

A Site-to-Site (S2S) VPN gateway connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. S2S connections can be used for cross-premises and hybrid configurations. A S2S connection requires a VPN device located on-premises that has a public IP address assigned to it. For information about selecting a VPN device, see the [VPN Gateway FAQ - VPN devices](#).

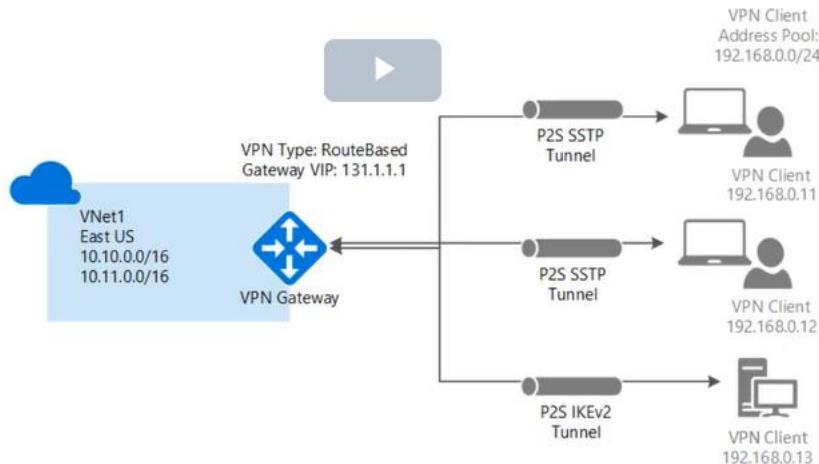


2. Point to Site VPN P2S – połączenie między stacjami klienckimi a Azure. Często stosowane przy pracy zdalnej. Ma ograniczoną przepustowość do 100Mbit. Nie jest skalowalne – można obsługiwać do 128 takich połączeń.

## Point-to-Site VPN

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

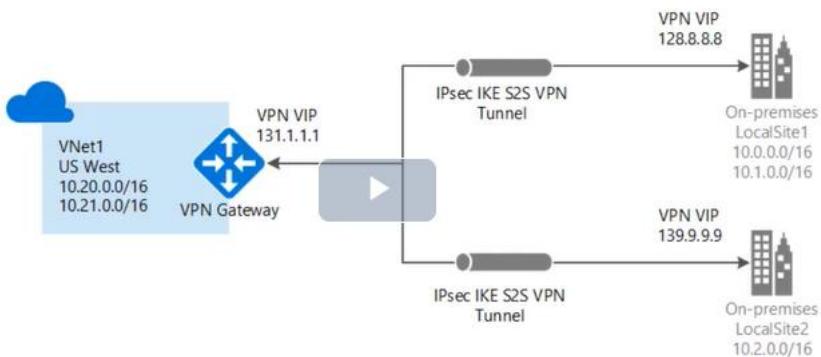
Unlike S2S connections, P2S connections do not require an on-premises public-facing IP address or a VPN device. P2S connections can be used with S2S connections through the same VPN gateway, as long as all the configuration requirements for both connections are compatible. For more information about Point-to-Site connections, see [About Point-to-Site VPN](#).



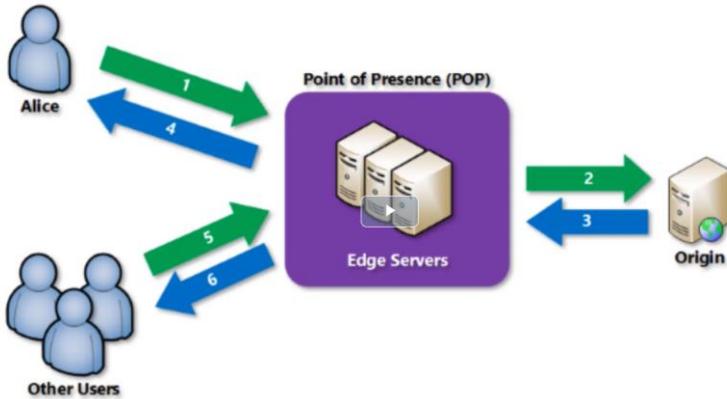
### 3. VNET to VNET – połączenie 2-ch sieci wirtualnych.

#### Multi-Site

This type of connection is a variation of the Site-to-Site connection. You create more than one VPN connection from your virtual network gateway, typically connecting to multiple on-premises sites. When working with multiple connections, you must use a RouteBased VPN type (known as a dynamic gateway when working with classic VNets). Because each virtual network can only have one VPN gateway, all connections through the gateway share the available bandwidth. This type of connection is often called a "multi-site" connection.

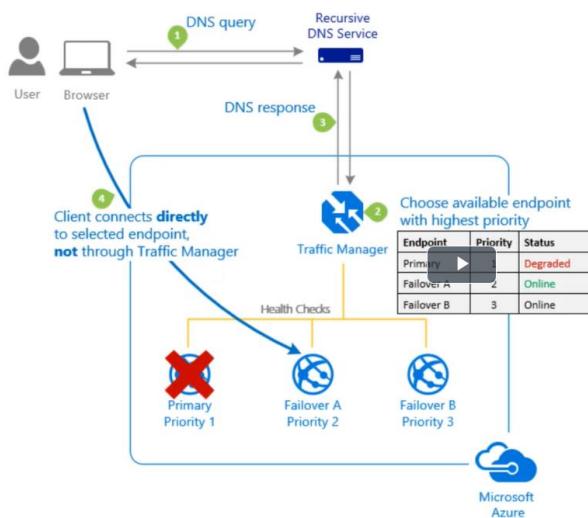


Kolejne rozwiązanie – Azure Content Delivery Network – organizuje efektywne przesyłanie danych po sieci.



Jeśli kolejny raz jest request po te same dane to są one pobierane nie ze źródła a z POP bo trafiły tam po pierwszym requeście. Każdy plik w POP ma time to leave po którym jest usuwany. Celem jest oszczędzanie na transferze danych na dużych odległościach.

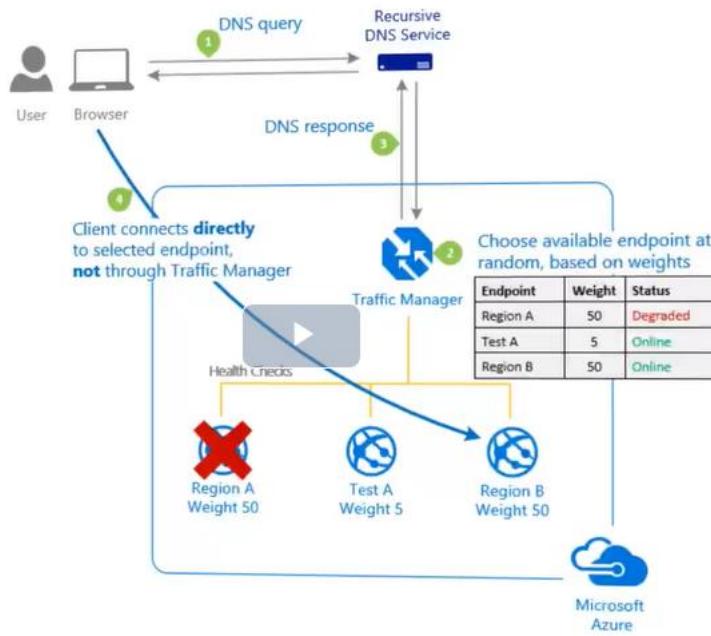
Azure Traffic Manager – ustala do jakich lokalizacji kierować requesty użytkownika. Zasoby są w wielu miejscach a ten manager kieruje tam, gdzie żądane dane mogą być pozyskane jak najszybciej. W tym przypadku nie dochodzi do transferu całego wielkiego pliku a pracujemy na DNSie. User prosi o zasób podając DNS a Manager przekierowuje go do odpowiedniej lokalizacji:



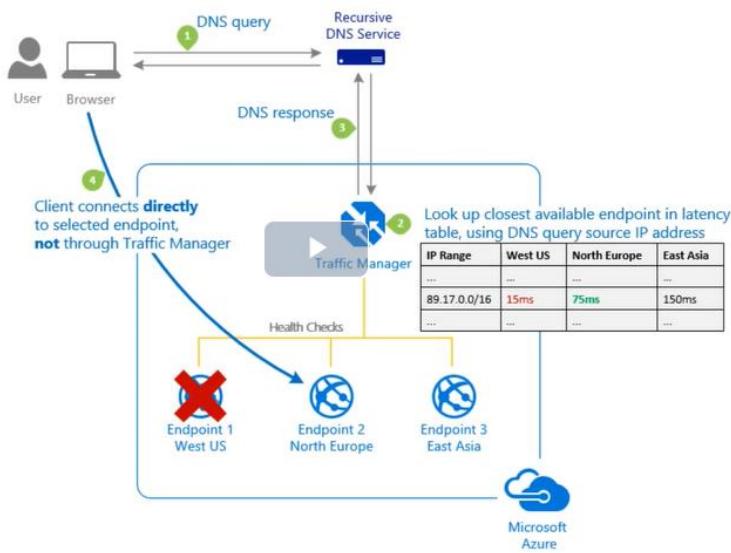
Istnieją reguły przekierowywania użytkownika:

**Priority** – określa, która lokalizacja jest priorytetowa i jeśli ona jest niedostępna to dopiero wtedy jest przekierowanie w inne miejsce.

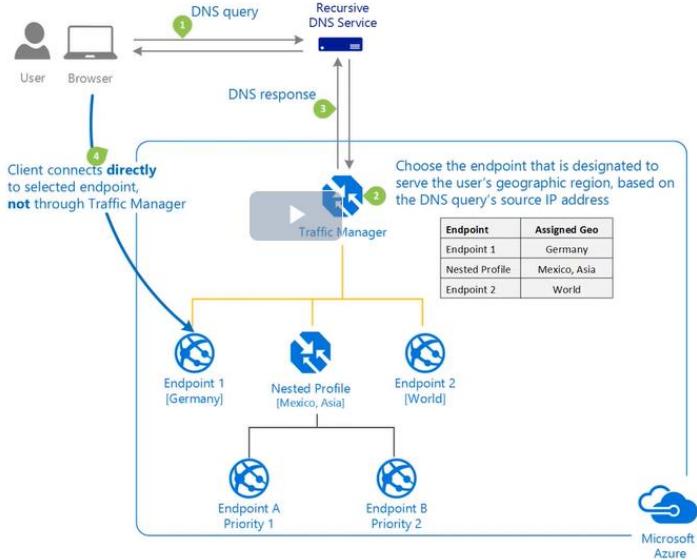
**Weighted** – dystrybuje pomiędzy różne lokalizacje danego zasobu. To która lokalizacja otrzyma więcej rządów zależy od przypisanych do tych lokalizacji wag



Performance – żądania są kierowane do tych endpointów, które mają najmniejsze opóźnienia sieciowe



Geography – użytkownik kierowany do najbliższej lokalizacji geograficznej



Multivalue - przekazuje całą listę endpointów i to po stronie klienta jest decyzja z którego zasobu chce skorzystać

### Budowa sieci: Virtual Network i Subnet

In depth defence – strategia budowania sieci. Bezpośrednio możemy dostać się tylko do pierwszej podsieci. Do kolejnej poprzez tą pierwszą i tak dalej...

Atak DDoS – Distributed Denial of Service – olbrzymie ilości zapytań (z wielu urządzeń) do konkretnego zasobu.

Definiując sieć określamy czy jaki poziom ochrony przed Ddos i czy chcemy firewalla:

The screenshot shows the Azure portal interface for creating a virtual network. The 'Security' tab is active, displaying options for DDoS protection (set to 'Basic') and Firewall (set to 'Disabled'). The left sidebar shows various Azure services like Home, Dashboard, and Resource groups.

Będziemy konfigurować połączenia między podsieciami. Do stworzonej sieci dodajemy ubuntu server. Dodajemy go w grupie zasobów:

https://portal.azure.com/#@deve4800-0011-40e1-ac43-181c971975c2/resource/subscriptions/08d2a365-709d-48b2-8fb4-7073703f4ec7/resourcegroups/restrictedrg/overview

Search resources, services, and docs (G+)

Home > Resource groups > RestrictedRG

### RestrictedRG

Resource group

Search (Ctrl+F) Add Edit columns Delete resource group Refresh Move Export to CSV Assign tags Delete Export template ...

Subscription (change) : Free Trial Deployments : 1 Succeeded

Subscription ID : 08d2a365-709d-48b2-8fb4-7073703f4ec7

Tags (change) : Click here to add tags

Filter by name... Type == all Location == all Add filter

Showing 1 to 1 of 1 records. Show hidden types

Name ↑	Type ↑↓	Location ↑↓
Restricted-VLAN	Virtual network	East US

No grouping

Overview Activity log Access control (IAM) Tags Events Settings Quickstart Deployments Policies Properties Locks Export template

Search resources, services, and docs (G+)

Home > Resource groups > RestrictedRG > New

### New

Search the Marketplace

Azure Marketplace See all Popular

- Get started
- Recently created
- AI + Machine Learning
- Analytics
- Blockchain
- Compute
- Containers
- Databases

Windows Server 2016 Datacenter  
Quickstarts + tutorials

Ubuntu Server 18.04 LTS  
Learn more

Web App  
Quickstarts + tutorials

SQL Database  
Quickstarts + tutorials

Search resources, services, and docs (Q+?)

Home > Resource groups > RestrictedRG > New > Create a virtual machine

### Create a virtual machine

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

**Subscription \*** ⓘ

**Resource group \*** ⓘ  [Create new](#)

**Instance details**

**Virtual machine name \*** ⓘ

**Region \*** ⓘ  [Change region](#)

**Availability options** ⓘ

**Image \*** ⓘ  [Browse all public and private images](#)

**Azure Spot instance** ⓘ  Yes  No

**Size \*** ⓘ **Standard D2s v3**  
2 vcpus, 8 GiB memory (€59.10/month)  
[Change size](#)

**Administrator account**

**Authentication type** ⓘ  SSH public key  Password

**Username \*** ⓘ

**Review + create** [< Previous](#) [Next : Disks >](#)

## Dotaczemy do pierwszej podsieci

Home > Resource groups > RestrictedRG > New > Create a virtual machine

### Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.  
[Learn more](#)

**Network interface**

When creating a virtual machine, a network interface will be created for you.

**Virtual network \*** ⓘ  [Create new](#)

**Subnet \*** ⓘ  [Manage subnet configuration](#)

**Public IP** ⓘ  [Create new](#)

**NIC network security group** ⓘ  None  Basic  Advanced

**Public inbound ports \*** ⓘ  None  Allow selected ports

**Select inbound ports \***

**⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.**

Home > Resource groups > RestrictedRG > New > Create a virtual machine

### Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Configure monitoring and management options for your VM.

**Azure Security Center**

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.  
[Learn more](#)

Your subscription is protected by Azure Security Center basic plan.

**Monitoring**

Boot diagnostics  On  Off

OS guest diagnostics  On  Off

Diagnostics storage account \*

**Identity**

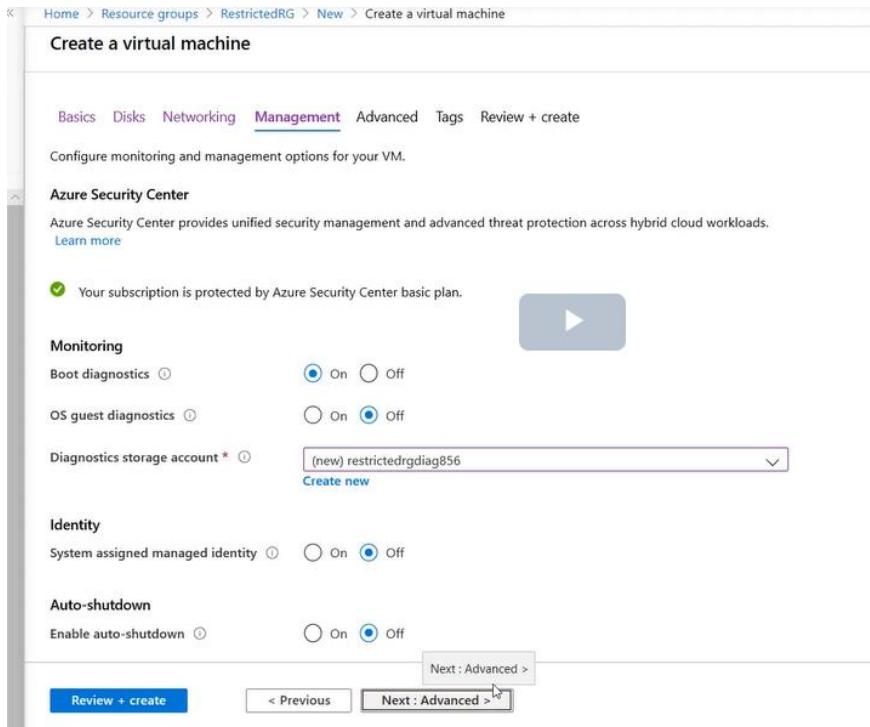
System assigned managed identity  On  Off

**Auto-shutdown**

Enable auto-shutdown  On  Off

**Next : Advanced >**

**Review + create** **< Previous** **Next : Advanced >**



Dodajemy kolejną maszynę wirtualną z Linuxem dla drugiej podsieci. Ale tym razem nie otwieramy portu publicznego:

Search resources, services, and docs (G+/)

Home > Resource groups > RestrictedRG > New > Create a virtual machine

### Create a virtual machine

**Size \***  Standard B1ms  
1 vcpu, 2 GiB memory (€12.74/month)  
[Change size](#)

**Administrator account**

Authentication type  SSH public key  Password

Username \*

Password \*

Confirm password \*

**Inbound port rules**

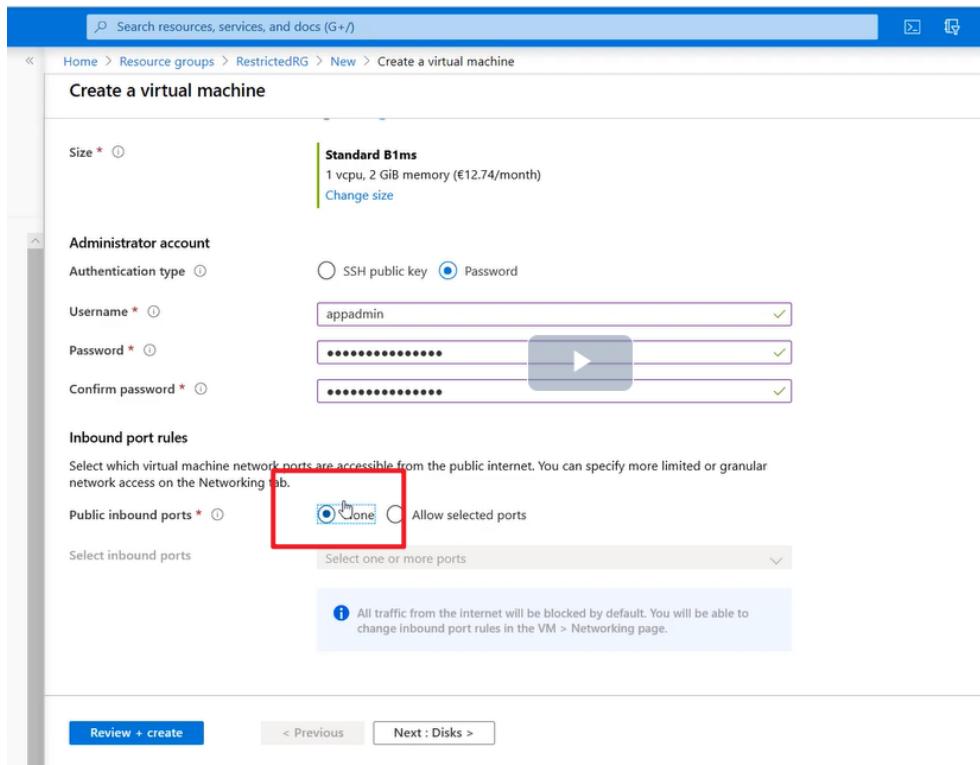
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*  Block all traffic  Allow selected ports

Select inbound ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

**Review + create** **< Previous** **Next : Disks >**



https://portal.azure.com/#create/microsoft.network/server-vm/network

Search resources, services, and docs (G+/)

Home > Resource groups > RestrictedRG > New > Create a virtual machine

### Create a virtual machine

Networking

Basics Disks Networking Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

Learn more

**Network interface**

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ Restricted-VLAN

Subnet \* ⓘ Subnet-B (10.1.2.0/24)

Public IP ⓘ None

NIC network security group ⓘ None Basic Advanced

Public inbound ports \* ⓘ None Allow selected ports

Select inbound ports Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Review + create < Previous Next : Management >

Trzecia maszyna tak samo:

https://portal.azure.com/#create/microsoft.network/server-vm/network

Search resources, services, and docs (G+/)

Home > Resource groups > RestrictedRG > New > Create a virtual machine

### Create a virtual machine

Size \* ⓘ Standard B1ms  
1 vcpu, 2 GiB memory (€12.74/month)

**Administrator account**

Authentication type ⓘ SSH public key Password

Username \* ⓘ appadmin

Password \* ⓘ

Confirm password \* ⓘ

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \* ⓘ None Allow selected ports

Select inbound ports Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Search resources, services, and docs (G+/)

Home > Resource groups > RestrictedRG > New > Create a virtual machine

## Create a virtual machine

Networking

Basics Disks Networking Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

**Network interface**

When creating a virtual machine, a network interface will be created for you.

Virtual network \*  [Create new](#)

Subnet \*  [Manage subnet configuration](#)

Public IP  [Create new](#)

NIC network security group  None  Basic  Advanced

Public inbound ports \*  None  Allow selected ports

Select inbound ports

Logujemy się do pierwszej maszyny wirtualnej korzystając z jej publicznego adresu IP. Sprawdzamy adres drugiej maszyny:

Home > Resource groups > RestrictedRG > srv02

**srv02** Virtual machine

Search (Ctrl+F)

Connect Start Restart Stop Capture Delete Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Networking Connect

Resource group (change) : RestrictedRG

Status : Running

Location : East US

Subscription (change) : Free Trial

Subscription ID : 08d2a365-709d-48b2-8fb4-7073703f4ec7

Computer name : srv02

Operating system : Linux (ubuntu 18.04)

Size : Standard B1ms (1 vcpus, 2 GB memory)

Tags (change) : Click here to add tags

Azure Spot : N/A

Public IP address : -

Private IP address : 10.1.2.4

Public IP address (IPv6) : -

Private IP address (IPv6) : -

Virtual network/subnet : Restricted-VLAN/Subnet-B

DNS name : -

Próbowiemy się połączyć z maszyną 1 do maszyny 2:

```
System load: 0.08 Processes: 107
Usage of /: 4.0% of 28.90GB Users logged in: 0
Memory usage: 17% IP address for eth0: 10.1.1.4
Swap usage: 0%
```

```
0 packages can be updated.
0 updates are security updates.
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
appadmin@srv01:~$ ssh appadmin@10.1.2.4
The authenticity of host '10.1.2.4 (10.1.2.4)' can't be established.
ECDSA key fingerprint is SHA256:8ueGzig9P0S4qkgvyGIBH2bF7RT8YeIXicAPHopV+cA.
Are you sure you want to continue connecting (yes/no)?
```

```
appadmin@srv02: ~
System information as of Wed Apr 22 22:25:24 UTC 2020
System load: 0.0      Processes: 108
Usage of /: 4.0% of 28.90GB  Users logged in: 0
Memory usage: 16%      IP address for eth0: 10.1.2.4
Swap usage: 0%
0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

appadmin@srv02:~$
```

Analogicznie logujemy się do sieci C. W sieci C możemy zalogować się do sieci A:

```
appadmin@srv03: ~
Memory usage: 16%          IP address for eth0: 10.1.3.4
Swap usage: 0%

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

appadmin@srv03:~$ ssh appadmin@10.1.1.4
The authenticity of host '10.1.1.4 (10.1.1.4)' can't be established.
ECDSA key fingerprint is SHA256:TjJkhNRFirzaVQVvkNA8+ANDJNQ0v/lsf7P5Vf5GGKU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.1.4' (ECDSA) to the list of known hosts.
appadmin@10.1.1.4's password: $
```

Tak samo z sieci A możemy bezpośrednio połączyć się do C. A nie chcemy tak.

W międzyczasie przesuniemy maszynę wirtualną z jednej do drugiej podsieci:

Jesteśmy podłączeni do sieci C:

Tu dokonujemy zmiany:

Zabezpieczamy sieć C:

W naszej resource grupie dodajemy:

The screenshot shows the Azure Marketplace search results for 'Network security group'. A blue dashed box highlights the 'Networking' category. The results list several services under 'Networking': Virtual network, CloudGuard IaaS - Firewall & Threat Prevention (preview), Load Balancer, Application Gateway, Front Door, Firewall, Virtual WAN, and Network security group. The 'Network security group' item is selected, showing its details: Resource group (change) : RestrictedRG, Location : East US, Subscription (change) : Free Trial, Subscription ID : 08d2a365-709d-48b2-8fb4-7073703f4ec7, and Tags (change) : Click here to add tags. It also displays 'Inbound security rules' and 'Outbound security rules'.

Ten obiekt reguluje ruch przychodzący i wychodzący:

The screenshot shows the Azure Network Security Group (NSG) overview page for 'NSG-C'. The left sidebar lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings', 'Inbound security rules', 'Outbound security rules', 'Network interfaces', 'Subnets', and 'Properties'. The main pane displays resource group information (Resource group (change) : RestrictedRG, Location : East US, Subscription (change) : Free Trial, Subscription ID : 08d2a365-709d-48b2-8fb4-7073703f4ec7, Tags (change) : Click here to add tags), custom security rules (0 inbound, 0 outbound), and associated subnets (0 subnets, 0 network interfaces). The 'Inbound security rules' table shows three rules:

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Reguły mają przypisane priorytety:

NSG-C Network security group

Resource group (change) : RestrictedRG Location : East US Custom security rules : 0 inbound, 0 outbound

Subscription (change) : Free Trial Associated with : 0 subnets, 0 network interfaces

Subscription ID : 08d2a365-709d-48b2-8fb4-7073703f4ec7

Tags (change) : Click here to add tags

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<span style="color: green;">Allow</span>
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	<span style="color: green;">Allow</span>
65500	DenyAllInBound	Any	Any	Any	Any	<span style="color: red;">Deny</span>

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	<span style="color: green;">Allow</span>
65001	AllowInternetOutBound	Any	Any	Any	Internet	<span style="color: green;">Allow</span>
65500	DenyAllOutBound	Any	Any	Any	Any	<span style="color: red;">Deny</span>

Priorytety nadajemy od wartości 100. 100 to priorytet najwyższy.

Definiujemy, że do sieci C możemy dostać się jedynie z sieci B:

Add inbound security rule  
NSG-C

Basic

Source \* ⓘ  
IP Addresses

Source IP addresses/CIDR ranges \* ⓘ  
10.1.2.0/24

Source port ranges \* ⓘ  
\*

Destination \* ⓘ  
IP Addresses

Destination IP addresses/CIDR ranges \* ⓘ  
10.1.3.0/24

Destination port ranges \* ⓘ  
22

Protocol \* ⓘ  
Any TCP UDP ICMP

Action \* ⓘ  
Allow Deny

Priority \* ⓘ  
100

Name \*

Dodajemy kolejną regułę, zabraniamy ruchu z innych IP:

The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). The top half displays the 'Add inbound security rule' dialog for an NSG named 'NSG-C'. The rule being created has the following parameters:

- Source:** Any
- Source port ranges:** \*
- Destination:** IP Addresses
- Destination IP addresses/CIDR ranges:** 10.1.3.0/24
- Destination port ranges:** \*
- Protocol:** Any
- Action:** Deny
- Priority:** 200
- Name:** Port\_8080

The bottom half shows the list of existing inbound security rules for the same NSG:

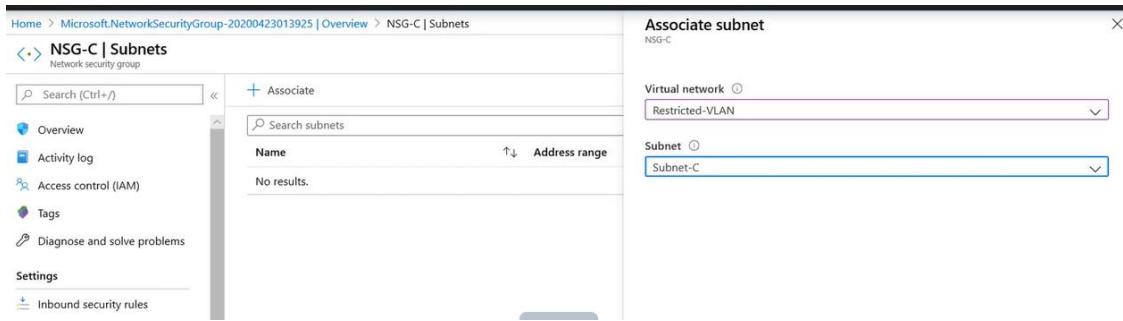
Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_SSH_From_B_To_C	22	TCP	10.1.2.0/24	10.1.3.0/24	Allow
200	Deny_All	Any	Any	Any	10.1.3.0/24	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

To były reguły przychodzące. Teraz robimy wychodzącą:

The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). On the left, the navigation pane is visible with sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Inbound security rules, Outbound security rules selected), Network interfaces, Subnets, Properties, Locks, Export template, Monitoring (Diagnostic settings, Logs, NSG flow logs), and Support + troubleshooting. The main content area shows 'NSG-C | Outbound security rules' with three existing rules: 'AllowVNetOutBound' (Priority 65000), 'AllowInternetOutBound' (Priority 65001), and 'DenyAllOutBound' (Priority 65500). A modal window titled 'Add outbound security rule' is open, showing fields for Source (Any), Source port ranges, Destination (Any), Destination port ranges, Protocol (Any selected), Action (Deny selected), Priority (100), Name (Deny\_All\_Outbound), and Description. A large blue 'Add' button is at the bottom right of the modal.

Musimy teraz regułę przypisać do podsieci albo do interfejsów sieciowych maszyn wirtualnych:

The screenshot shows the 'NSG-C | Subnets' page within the NSG configuration. The left sidebar has the same navigation options as the previous screenshot. The main area displays a table with one row: 'No results.' Under the 'Name' column. Above the table, there is a search bar labeled 'Search subnets' and a large blue button labeled '+ Associate'. The 'Subnets' option in the left sidebar is highlighted with a red box.



## Coś dla programistów – Azure DevOps

Azure Devops to zbiór rozwiązań które mają wspierać pracę programisty. Do dyspozycji są takie produkty jak:

1. Azure Boards – zbiór narzędzi raportujących do śledzenia pracy programisty – dla nadzorujących. Konfigurowalne elementy na których można umieszczać graficzne obiekty.
2. Azure Pipelines – pozwala na wykonywanie CI/CD.
3. Azure Repos – pozwala na przechowywanie i zarządzanie kodem źródłowym aplikacji
4. Azure Test Plans – do zarządzania testami
5. Azure Artifacts – biblioteki z których mogą korzystać programiści. Pobieramy te biblioteki i z nich korzystamy – na wypadek gdyby zniknęły z internetu
6. Extensions Marketplace – rozszerzenia, które można włączyć podczas tworzenia aplikacji

## Azure Dev Test Labs

Azure Dev Test Labs pozwala zapanować nad procesem testowania. W ramach środowiska można mieć do dyspozycji przygotowane obrazy maszyn wirtualnych, które wystarczy wdrożyć. Dla firm, które nie chcą się przejmować przygotowywaniem środowisk testowych. Tam gdzie jest wiele komponentów, różnorakie systemy. Środowiska testowe służą nie tylko do weryfikacji poprawności działania ale też do badania wydajności. Jeśli środowisko produkcyjne znajduje się na Azure to środowisko testowe może być wierną kopią danych z produkcji. Możemy też weryfikować jakie koszty niesie za sobą utrzymanie takiego środowiska. Stworzenie samego Dev Test Laba jest za darmo ale trzeba będzie płacić za utworzone tam zasoby – dyki, maszyny wirtualne

## Azure Functions

Można wdrożyć rozwiązania, które będą działały ale nie otrzymają na własność maszyny wirtualnej. W Microsoftie jest dużo wyłączonych maszyn, których potencjał się marnuje. Przykładem rozwiązania serverless jest Azure patches.

Microsoft Azure

Home - Microsoft Azure | https://portal.azure.com/#home

function

Services

- Function App
- Image definitions
- Service catalog managed application definitions
- App Services

Resources

No results were found.

Marketplace

- Function App
- MAKANA Python Function

Documentation

- Azure Functions custom handlers (preview) | Microsoft Docs
- User-Defined Functions - Azure Data Explorer | Microsoft Docs
- Azure Functions HTTP trigger | Microsoft Docs
- Stored functions management overview - Azure Data Explorer...

Resource Groups

No results were found.

Subscriptions

Policy

More services

Last Viewed

3 days ago
3 days ago
3 days ago
3 days ago

Search all subscriptions. Change

RestrictedRG

srv01-nsg

Network security group

This screenshot shows the Microsoft Azure portal's home page. A search bar at the top contains the text 'function'. Below the search bar, there are sections for 'Services' and 'Resources'. The 'Services' section lists 'Function App', 'Image definitions', 'Service catalog managed application definitions', and 'App Services'. The 'Resources' section shows a message 'No results were found.' To the right, there is a 'Marketplace' section with links to 'Function App' and 'MAKANA Python Function', and a 'Documentation' section with links to various Azure Functions documentation pages. At the bottom, there are sections for 'Subscriptions', 'Policy', and 'More services', along with a 'Last Viewed' table showing items last viewed 3 days ago. A message at the bottom says 'Search all subscriptions. Change'.

Function App - Microsoft Azure | https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Web%2Fsites/kind/functionapp

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Function App

Function App

Default Directory

Add Manage view Refresh Export to CSV Assign tags Start Restart

Filter by name... Subscription == all Resource group == all Location == all

Showing 0 to 0 of 0 records.

Name ↑↓	Status ↑↓	Location ↑↓
---------	-----------	-------------

Play icon

This screenshot shows the 'Function App' blade in the Microsoft Azure portal. The URL in the address bar is 'https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Web%2Fsites/kind/functionapp'. The page title is 'Function App - Microsoft Azure'. The left sidebar includes a 'Function App' item under 'App Services'. The main content area is titled 'Function App' and 'Default Directory'. It features a toolbar with 'Add', 'Manage view', 'Refresh', 'Export to CSV', 'Assign tags', 'Start', and 'Restart' buttons. Below the toolbar is a filter bar with fields for 'Filter by name...', 'Subscription == all', 'Resource group == all', and 'Location == all'. A message below the filter bar says 'Showing 0 to 0 of 0 records.'. At the bottom, there is a table header with columns for 'Name ↑↓', 'Status ↑↓', and 'Location ↑↓'. A play button icon is located at the bottom right.

https://portal.azure.com/#create/Microsoft.FunctionApp

**Project Details**

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

**Subscription \*** Free Trial

**Resource Group \*** (New) ServerlessRG

**Instance Details**

**Function App name \*** GreetingService

**Publish \*** Code

**Runtime stack \*** .NET Core

**Version \*** 3.1

**Region \*** Central US

**Review + create** < Previous Next : Hosting >

**GreetingService**

All subscriptions

Function Apps

GreetingService

Status: Running

Subscription: Free Trial

Resource group: ServerlessRG

URL: https://greetingservice.azurewebsites.net

Configured features

Function app settings

Configuration

You have created a function app!

Now it is time to add your code...

+ New function

Teraz musimy określić jak funkcja ma się uruchomić:

Webhook – funkcja wykona się gdy ktoś odwoła się do adresu url.

```

    run.csx
    Save     Save and run   </> Get function URL

    1 #r "Newtonsoft.Json"
    2
    3 using System.Net;
    4 using Microsoft.AspNetCore.Mvc;
    5 using Microsoft.Extensions.Primitives;
    6 using Newtonsoft.Json;
    7
    8 public static async Task<ActionResult> Run(HttpContext req, ILogger log)
    9 {
        log.LogInformation("C# HTTP trigger function processed a request.");
    10
    11     string name = req.Query["name"];
    12     name = name.ToUpper();
    13
    14     // string requestBody = await new StreamReader(req.Body).ReadToEndAsync();
    15     // dynamic data = JsonConvert.DeserializeObject(requestBody);
    16     // name = name ?? data?.name;
    17
    18     return name != null
    19         ? (ActionResult)new OkObjectResult($"Hello, {name}")
    20         : new BadRequestObjectResult("Please pass a name on the query string or in the request body");
    21
    22 }
    23
  
```

Jest to zasób zwany serverless bo do uruchomienia funkcji nie trzeba było konfigurować swojego serwera wirtualnego.

## Logic App

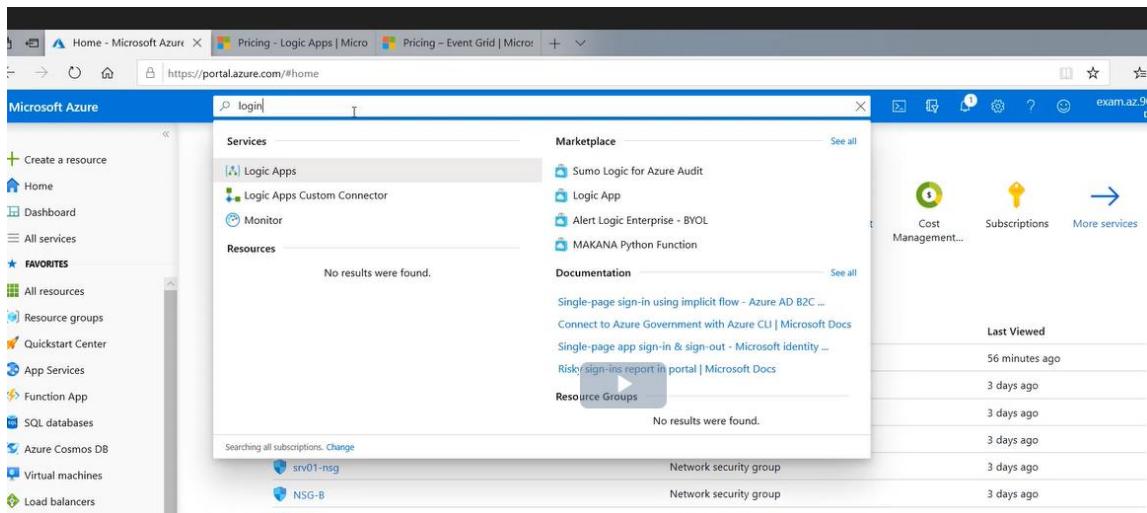
Kolejny przykład funkcji serverless.

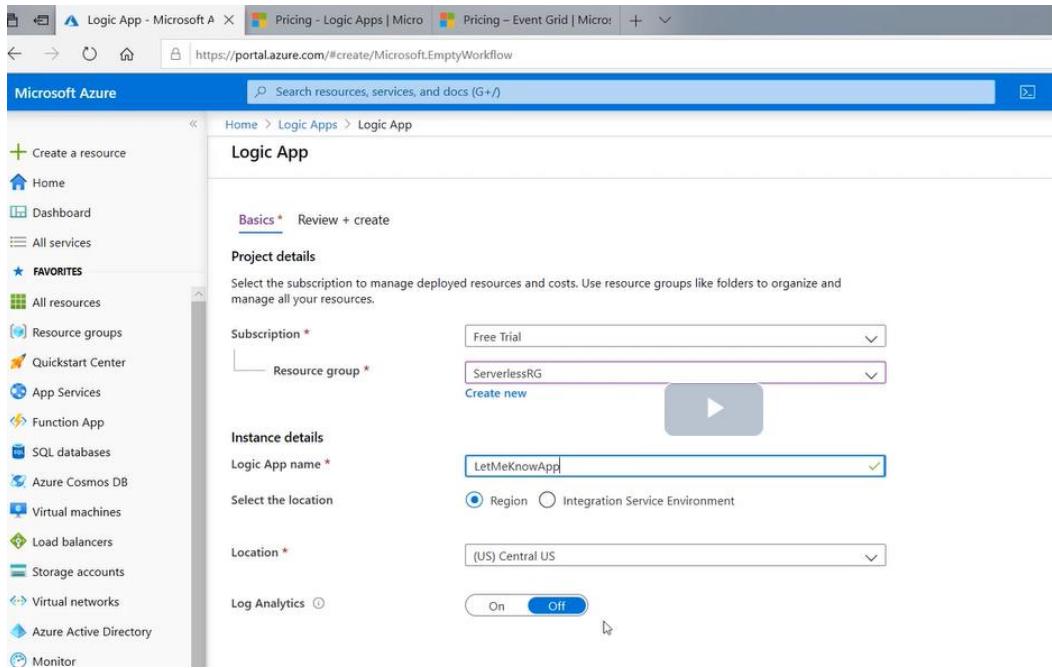
1 cecha Logic App – tworzenie aplikacji polega na przeciąganiu komponentów i uzupełnianiu ich parametrów

2 cecha – nadaje się do budowania aplikacji które automatyzują pracę administratora Azure. Nadaje się do integracji Azure a częścią aplikacji są permissions.

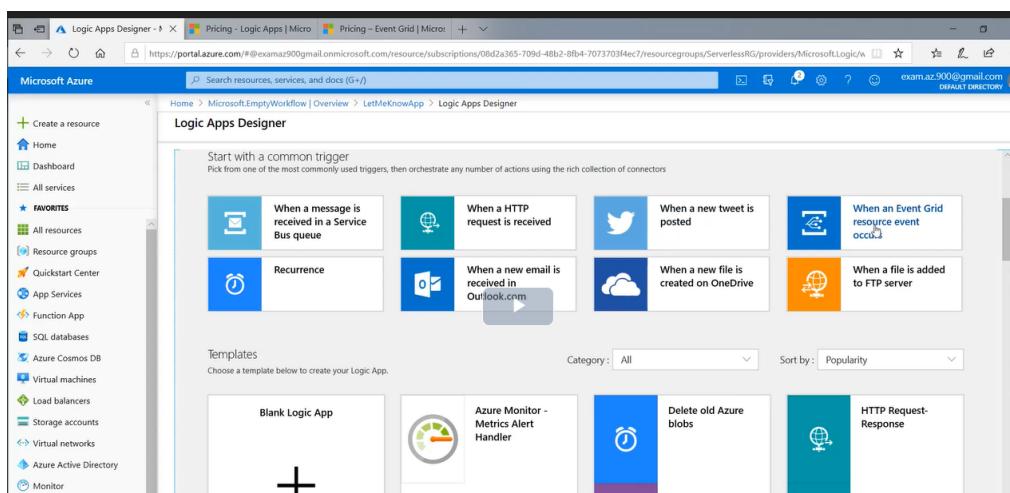
Budujemy mechanizm, który będzie powiadniał o zmianach w wybranej resource grupie. W tym celu skorzystamy z obiektu, który nazywa się Event Grid.

Event Grid – to serwis, który otrzymuje informacje o wszystkich zdarzeniach w Azure.



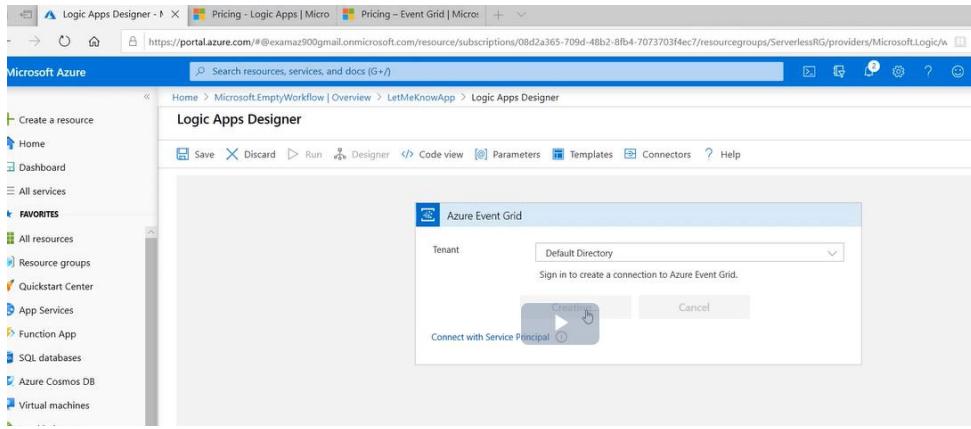


Wybieramy co ma wzbudzić Logic App:

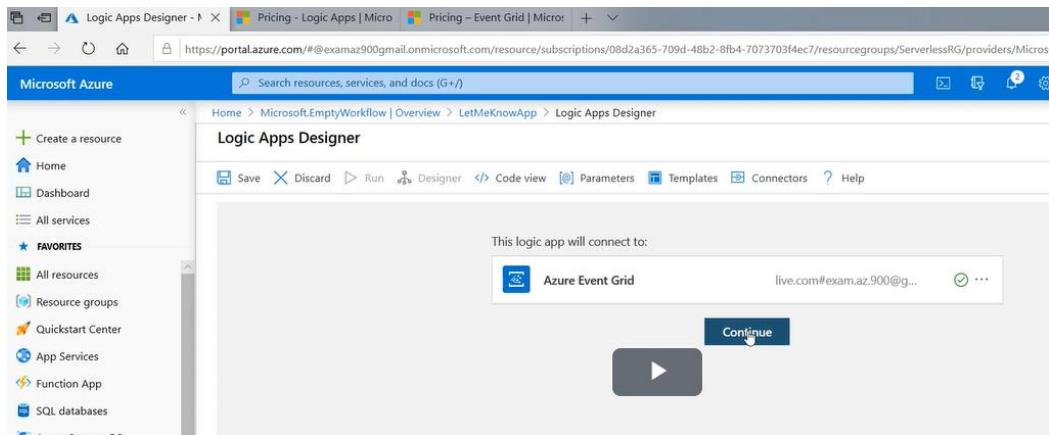


Wybieramy zdarzenie, które pojawiło się w event gridzie.

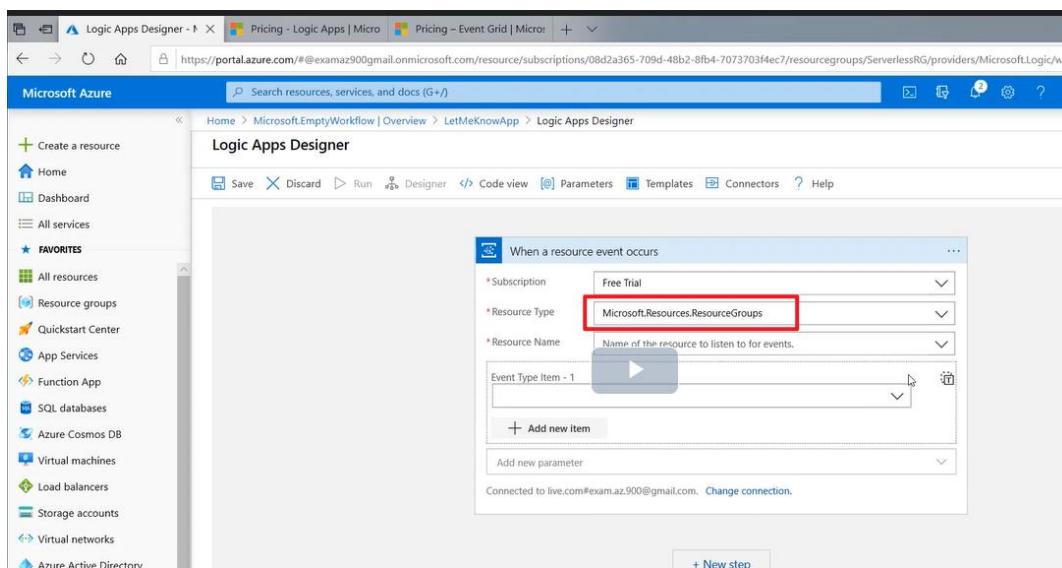
Łączymy się z event gridem:



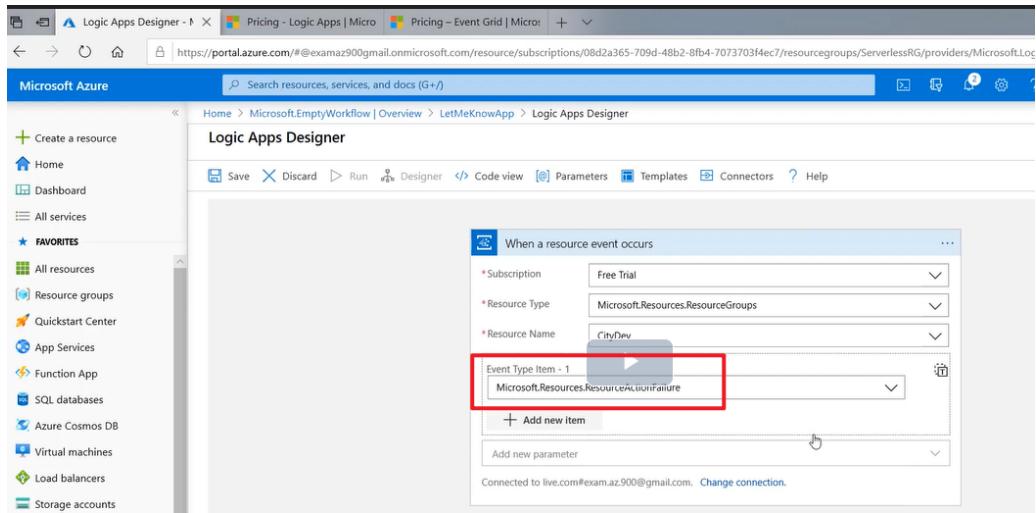
Połączenie odbywa się w domyślnym katalogu. Wykorzystujemy konto Azure:



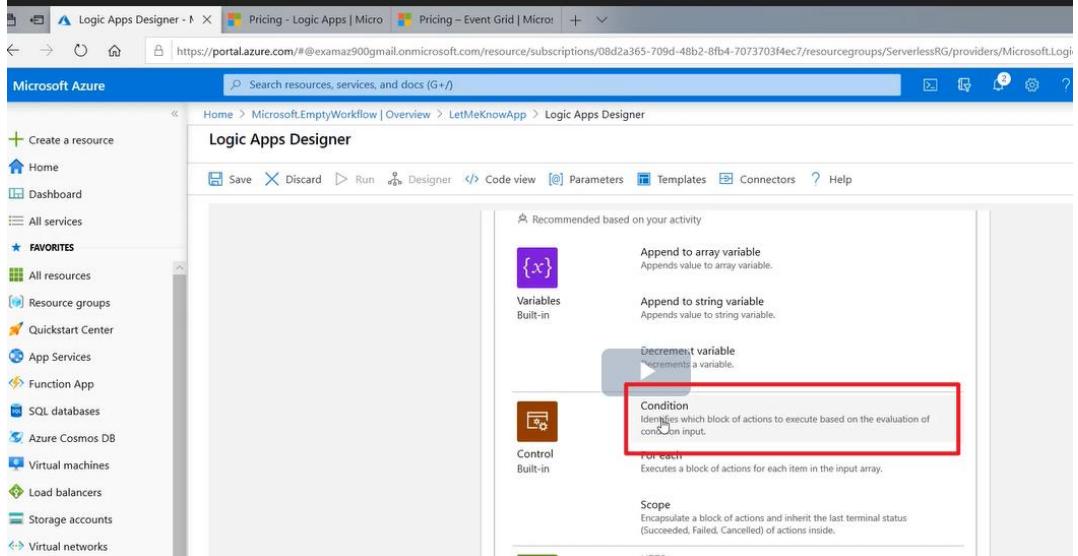
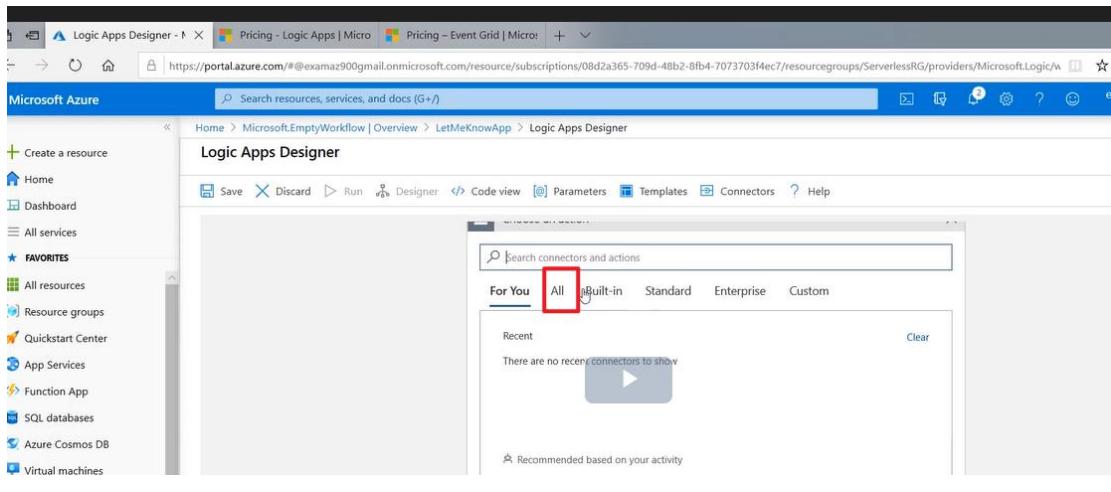
Określamy jakie zdarzenia są dla nas interesujące. Interesują nas zdarzenia z Resource grupy:



Wybieramy jakie enemy nas interesują:



Chcemy żeby wykonało się sprawdzenie:



Robimy sprawdzenie z jakiego rodzaju operacją mamy do czynienia:

The screenshot shows the Azure Logic Apps Designer interface. At the top, there's a navigation bar with tabs like 'Code view', 'Parameters', 'Templates', 'Connectors', and 'Help'. The main workspace contains a workflow with a trigger 'if VM was changed' followed by a condition 'And' block. A modal window is open over the workspace, titled 'Expression', containing the code `fx triggerBody()?['data'][ 'operationName']`. Below the expression, there's a button labeled 'OK'. In the bottom right corner of the modal, there's a link 'String functions' with a 'See more' button. The background of the designer shows other parts of the logic app, including a 'Condition' block with an 'If true' path and an 'If false' path.

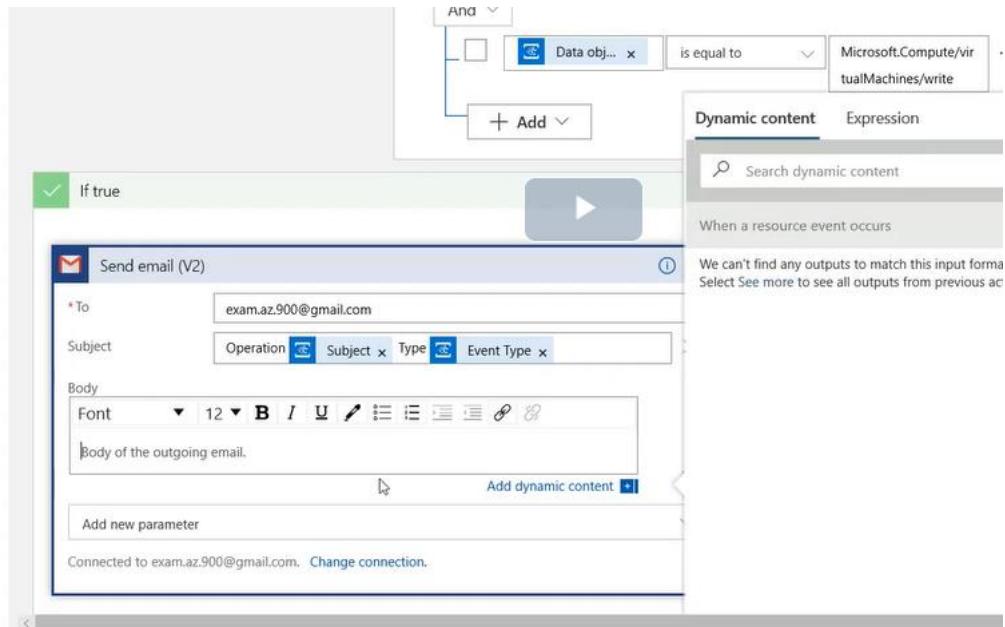
Jeśli takie zdarzenie będzie miało miejsce to chcę zostać o tym powiadomiony

<https://portal.azure.com/#@examaz900@gmail.onmicrosoft.com/resource/subscriptions/08d2a365-709d-48b2-8fb4-7073703f4ec7/resourceGroups/EmptyWorkflow/providers/Microsoft.Logic/workflows/EmptyWorkflow>

The screenshot shows the Logic Apps Designer interface. At the top, there's a search bar and a breadcrumb navigation: Home > Microsoft.EmptyWorkflow | Overview > LetMeKnowApp > Logic Apps Designer. Below the header, there's a toolbar with Save, Discard, Run, Designer, Code view, Parameters, Templates, Connectors, and Help buttons. The main area is titled 'Logic Apps Designer' and has a sub-header 'Actions'. A search bar at the top of this section contains the text 'send email'. Below it, there are tabs for 'For You', 'All', 'Built-in', 'Standard', 'Enterprise', and 'Custom'. Under the 'All' tab, several actions are listed under the 'Gmail' connector, including 'Delete email', 'Get email details', 'Move email to trash', 'Reply to email (V2)', and 'Send email (V2)'. The 'Send email (V2)' action is currently selected.

The screenshot shows the Logic Apps Designer interface with a more complex workflow. At the top, there's a search bar and a breadcrumb navigation: Home > Microsoft.EmptyWorkflow | Overview > LetMeKnowApp > Logic Apps Designer. Below the header, there's a toolbar with Save, Discard, Run, Designer, Code view, Parameters, Templates, Connectors, and Help buttons. The main area is titled 'Logic Apps Designer' and shows a workflow editor. A condition block is at the top, with a condition: 'And' followed by 'Data obj... is equal to Microsoft.Compute/virtualMachines/write'. Below this, there are two branches: 'If true' and 'If false'. The 'If true' branch contains a 'Gmail' action block with 'Authentication Type' set to 'Use default shared application' and a 'Sign in' button. The 'If false' branch contains a placeholder 'Add an action' block.

Logujemy się do maila, uzupełniamy treść wiadomości jaka ma się wysyłać:



Przechodzimy do resource grupy i tworzymy maszynę wirtualną. Jeśli mail się nie wyśle to trzeba sprawdzić resource providers naszej subskrypcji:

Resource Provider	Cost (EUR)
cloudvhm.disk.0ef0db23c94ed85...	1.17 EUR
cloudvhm.9915	0.17 EUR
Others	0.05 EUR
Support + troubleshooting	0.01 EUR

The screenshot shows the Azure portal interface. In the top navigation bar, there are tabs for 'Connectors for Azure Logic', 'Pricing - Logic Apps | Micro', and 'Pricing - Event Grid | Micro'. The main content area is titled 'Free Trial | Resource providers'. On the left, there's a sidebar with 'source' and 'Billing' sections. Under 'Billing', there are links for 'Invoices', 'External services', 'Payment methods', and 'Partner information'. Below that is a 'Settings' section with 'Programmatic deployment' and 'Resource groups'. The main pane has a search bar at the top with 'event' typed in. To the right of the search bar are 'Register', 'Unregister', and 'Refresh' buttons. A table lists two resource providers: 'Microsoft.EventGrid' and 'Microsoft.EventHub', both with a status of 'NotRegistered'. A large blue play button is centered below the table.

Po tym trzeba przejść do Logic App a następnie wyłączyć i włączyć apkę:

The first part of the screenshot shows the Azure search bar with 'logic a' typed in. Below it, the search results are displayed under the 'Services' category, with 'Logic Apps' being the selected item. The second part of the screenshot shows the 'LetMeKnowApp' Logic App overview page. The app name 'LetMeKnowApp' is highlighted with a red box. Below it, there are buttons for 'Run Trigger', 'Edit', 'Delete', and 'Enable'. The 'Enable' button is also highlighted with a red box. The status of the app is shown as 'Successfully disabled logic app'.

Na karcie overview mamy informację o tym ile razy został uruchomiony trigger:

Status	Start time	Identifier	Duration	Static Results
Succeeded	4/25/2020, 6:18 PM	0858613775370581805238724312CU05	564 Milliseconds	
Succeeded	4/25/2020, 6:18 PM	08586137753866436539159677950CU23	320 Milliseconds	
Succeeded	4/25/2020, 6:17 PM	08586137754067097956685536003CU09	418 Milliseconds	
Succeeded	4/25/2020, 6:17 PM	08586137754176047119771458873CU18	313 Milliseconds	
Succeeded	4/25/2020, 6:17 PM	08586137754574108365238217947CU03	306 Milliseconds	
Succeeded	4/25/2020, 6:16 PM	08586137754988029545324990261CU07	321 Milliseconds	
Succeeded	4/25/2020, 6:16 PM	08586137755203827694400844727CU08	149 Milliseconds	
Succeeded	4/25/2020, 6:16 PM	08586137755210501023262214893CU01	647 Milliseconds	

## Windows Virtual Desktop – Desktop as a Service

Windows Virtual Desktop to technika przeniesienia aplikacji do chmury ale w całości – łącznie z urządzeniami klienckimi. Kolejny krok w wirtualizacji – zwirtualizowaliśmy serwery, bazy danych – teraz pora na aplikacje klienckie. Zalety:

- sprzęt nie musi być już tak często aktualizowany
- nie ma sytuacji, że w aplikacji coś nie działa
- wszystko odbywa się centralnie (aplikacja i virtual desktop w jednym miejscu) – jest bezpieczniej, nie ma problemu, że ktoś nam ukradnie komputer
- rozwiązanie zgodne z certyfikatami – nie trzeba ogarniać tego samodzielnie

Na jednej maszynie może pracować więcej użytkowników – wtedy mamy multisesyjność.

Windows Virtual Desktop przesuwa punkt ciężkości rozwiązyania klienckiego z maszyny użytkownika w stronę centralnej lokalizacji, gdzie tak na prawdę odbywa się całe przetwarzanie aplikacji. W takiej konfiguracji stacja robocza nie musi posiadać zbyt wielu zasobów, bo praktycznie odpowiada tylko za pobieranie danych od użytkownika i wyświetlanie informacji. Taka konfiguracja jest często nazywana "thin client" (cienki klient). Przeciwieństwem jest "fat client" (gruby klient).

## Container Instances i Azure Kubernetes

Nowe trendy w budowaniu aplikacji jest budowanie kontenerów.

W przypadku Virtual machines na jednym komputerze mamy system operacyjny i na tym systemie operacyjnym następne systemy operacyjne dla maszyn wirtualnych. Jeśli mamy 5 maszyn na jednym serwerze to znaczyło, że trzeba było przewidzieć zasoby dla w sumie 6 maszyn.

W przypadku konferencji na systemie operacyjnym mamy tylko jeden zasób do obsługi różnych aplikacji. Kontener budujemy w taki sposób, że do podstawowego obrazu maszyny wirtualnej dodajemy wszystko to co charakteryzuje daną aplikację. W przypadku kontenerów użycie zasobów jest zdecydowanie mniejsze. Wystarczy na docelowy komputer skopiować skonteneryzowaną aplikację i ją uruchomić bo sam kontener ma wszystko co potrzeba do uruchomienia aplikacji.

Azure Container Instances jest traktowany jako PaaS – maszyna uruchamia kontener. Płacisz za zasoby jakie przez ten kontener są konsumowane.

Azure Kubernetes Service – dla wielkich aplikacji mających duże obciążenia. Kubernetes zarządza kontenerami. Skonfigurowanie Kuberntesa on permises to nie lada zadanie. W Azure wyklikujemy opcje. Kubernetes grupuje kontenery w pody. Kontenery z jednego poda mogą współdzielić zasoby. Każdy pod ma swoje własne zasoby. Komputer na którym działają pody to worker albo node. | Duże rozwiązania wymagają dużej ilości nodów. W takim przypadku nody te są nadzorowane przez mastera i taka konfiguracja to Kubernetes Klaster.

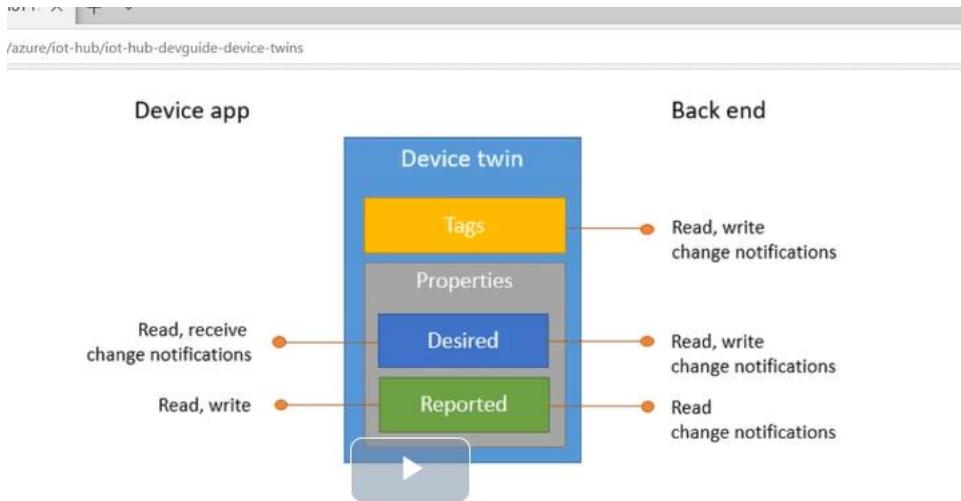
Sam Azure Kubernetes Service nie jest płatny ale jego zasoby tak.

## **Internet of Things**

Budowanie rozwiązań gdzie dużo czujników raportuje w jedno miejsce. Np. zarządzanie klimatyzacją w wielkim budynku.

Narzędzia Azure wspierające IoT:

- Azure IoT Hub – ma odpowiadać za nawiązywanie komunikacji z urządzeniami i odbieranie informacji, które z nich przychodzą. Możemy tu zarejestrować do miliona urządzeń. W IoT Hub można wysyłać komunikaty do urządzeń i takie komunikaty nazywa się Cloud To Device albo CtoD albo od urządzenia do huba (Device to Cloud). Możemy decydować co się dzieje z takimi przychodząymi wiadomościami – mogą trafiać do event huba ale możemy też je kierować na storage. W IoT hub jest klucz zabezpieczający komunikację. Jest też plik twin. Jest to plik json skojarzony z każdym urządzeniem, które jest zainstalowane. Składa się z wielu części np. tagi – urządzenia mające ten sam tag cechują się wspólnymi cechami i możemy hurtowo sterować urządzeniami. Inna sekcja to reported – ustawienia urządzenia jakie teraz to urządzenie posiada. Inna sekcja to desired – to co zostało zaprojektowane przez administratora dla danego urządzenia.



IoT Hub ma serwis Device provisioning service – wstępna konfiguracja urządzeń dołączanych do infrastruktury.

Azure IoT Central – w tym przypadku mniej skupiamy się na komuniakacji. Chodzi o wyciąganie biznesowej wartości z IoT. Chodzi nie tylko o zbieranie komunikatów ale też do wysyłanie ich do aplikacji które z nich korzystają np. do PowerBI. Azure IoT Central to SaaS.

Azure Sphere – dotyczy bezpieczeństwa samych czujników. W przypadku Azure Sphere Microsoft zbudował własny system operacyjny, który może być instalowany na tych urządzeniach. System jest podzielony na warstwy dzięki czemu możliwy jest defence in depth. Nie trzeba kierować się do dostawcy urządzeń po aktualizacje tylko ogarnia to Microsoft. Urządzenia też ogarnia Microsoft.

## Bazy danych w Azure

Azure SQL Database – baza danych MS SQL Server w chmurze. Mamy 3 rozwiązania:

- Single – użytkownik dostaje endpoint do podłączenia bazy danych, która jest gdzieś w chmurze. Możemy płacić DTU – database transaction unit (płatenie za transakcje) albo zdecydować się na virtual core model – stała opłata.
- Elastic Pool – do dyspozycji jest kilka baz danych na jednym serwerze. Wspólne zasoby mają bazy danych.
- Managed Instance – kompatybilne z implementacją SQL Servera on premises. Główne po to się to stosuje żeby migrować z on premises do chmury.

Azure Database Migration Service – serwis do migracji z on premises do chmury w wygodny sposób. Pozwala wybrać co ma być migrowane i synchronizuje zmiany jakie są w azure.

Azure Cosmos DB – nierelacyjna baza danych. 4 sposoby przechowywania danych: klucz/wartość, system kolumnowy, dokumentowa baza danych, grafowa baza danych

Interfejsy programistyczne API do pracy z bazą danych:

- SQL (Core) API – zwykłe zapytania
- Cassandra API – baza danych kolumnowa
- Azure Cosmos DB API for MongoDB – dla bazy danych dokumentowej
- Table API – interfejs do CosmosDB
- Gremlin API – baza danych grafowa

Azure Database for MySQL – Azure dla MySQL. Dla PostGres też działa.

### **Big Data w Azure**

Aktualnie gdy mamy dyski 1 TB to za Big Data uznajemy 1 PB. Big data jest wtedy gdy nie da się przetworzyć przez komputer danych bo jest ich za dużo.

Azure Synapse Analytics – dane są przechowywane w postaci relacyjnej ale są przetwarzane przez wiele serwerów i dzięki temu mamy szybko wyniki. Można nadawać uprawnienia userom, dane są szyfrowane – więc jest bezpieczne. Żeby uzyskać dane z Azure Synapse trzeba napisać zapytanie SQL. W przypadku Big Data problematyczne jest nie tylko odczytywanie danych ale i ładowanie. Dlatego mamy programy ADF copy albo SSIS albo zapytań kierowanych innych baz przy pomocy których dane są ładowane do Azure Synapse. W Azure Synapse jest cachowane elementów żeby przyspieszyć działanie zapytań. Przetwarzanie odbywa się na wielu klastrach.

Data lake to zbiór danych w postaci nieustrukturyzowanej.

Azure Data Lake Storage – produkt do pracy z Data Lake. Mamy 2 generacje storage.

Gen 1. – przechowywanie danych w postaci binary large object. Struktura danych jest płaska

Gen. 2 – pozwala na grupowanie blobów. Przetwarzanie może być łatwiejsze bo możemy przetwarzać dane jednego katalogu. Ten storage jest bardziej wydajny. Mamy różne opcje storagów:

	<b>Premium performance</b>	<b>Hot tier</b>	<b>Cool tier</b>	<b>Archive tier</b>
<b>Availability</b>	99.9%	99.9%	99%	Offline
<b>Availability (RA-GRS reads)</b>	N/A	99.99%	99.9%	Offline
<b>Usage charges</b>	Higher storage costs, lower access and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
<b>Minimum object size</b>	N/A	N/A	N/A	N/A
<b>Minimum storage duration</b>	N/A	N/A	30 days <sup>1</sup>	180 days
<b>Latency (Time to first byte)</b>	Single-digit milliseconds	milliseconds	milliseconds	hours <sup>2</sup>

W przypadku Archive mamy dostęp do danych z dużym opóźnieniem. Nadaje się do danych archiwanych.

HDInsight – dane mają być przetwarzane w prosty sposób z niewielkim kosztem. Budowane są klastry serwerów i gdy pojawiają się zadania do przetworzenia zarządcą kieruje te zadania do nodów w klastrach. Praca rozproszona. Każdy z nodów wykonuje pewien kawałek pracy.

Azure Databricks – pretwarzanie danych w trybie serverless computing. Nie mamy dedykowanych maszyn. Gdy coś potrzebujemy przetworzyć to wtedy jest oddawana do dyspozycji moc obliczeniowa. Azure Databricks to zbiór narzędzi przy pomocy których możemy projektować w jaki sposób dane będą wytwarzane. Budujemy skrypty, programy joby. Nie oczekujemy, że dane zostaną otrzymane natychmiast.

Jako że to jest serverless to nie płacimy za zasoby zarezerwowane a jedynie za czas realizacji zadań.

czy wiesz, że Big Data jest czasami definiowane za pomocą 3V (trzech V)?

volume - ilość

velocity - prędkość

variety - różnorodność

czy wiesz, że mamy 4 główne etapy pracy z danymi Big Data:

pobieranie ze źródeł danych

integracja i przechowywanie

analiza i modelowanie

wizualizacja i raportowanie

### **Machine Learning – wprowadzenie**

Machine Learning – wcześniej nie było wystarczającego storagu ani mocy obliczeniowej dlatego implementacja ML rozwija się dynamicznie dopiero teraz.

Przykład machine learning – wynajmowanie pokoju. Jeśli ktoś zgłosi się z pokojem do wynajęcia to algorytm ML ustali jaka powinna być cena za ten wynajem.

Dzieje się to tak, że algorytm analizuje dostępne dane. W oparciu o te dane znajduje najważniejsze zależności np. Wyposażenie, rok oddania pokoju itd. Algorytmy analizując olbrzymią ilość informacji, analizują je i uczą się rozpoznawać to co jest najbardziej istotne. W ten sposób powstaje model. Model zawiera wyrażenia matematyczne, które pozwalają na ustalenie proponowanej ceny.

Możemy zbudować model lokalnie. Ale możemy używać Azure Notebooks.

W przypadku Azure Machine Learning możemy dostarczyć dane z naszego komputera. Oczyszczamy dane i dzielimy je na dwie grupy – część uczącą i część testową. Część ucząca służy algorytmowi do szukania powiązań między cechami danych a część testowa do oceny modelu.

Jeśli korzystamy Azure Machine Learning to znowu korzystamy z usługi serverless bo nie mamy dedykowanych maszyn. Jak model jest zbudowany to możemy go wyeksportować w postaci kontenera Dockera.

### **Machine Learning w Azure**

Azure Machine Learning – przy użyciu tego programu możemy tworzyć własne algorytmy w sposób graficzny.

Przy korzystaniu z Machine Learning Studio mamy do dyspozycji bloki odpowiadające za różne czynności. Bloki przeciąga się an panel skryptów i łączy się ze sobą.

Azure Bot Service – pozwala na tworzenie oprogramowania które pozwala na prowadzenie rozmowy z klientem. Np czat wbudowany w stronę webową. Azure Bot Service odpowiada na potrzebę integracji ze środowiskiem interakcji z użytkownikiem, np ze slackiem albo messengerem. Sam bot jest pisany w języku programowania.

Integracja z Microsoftowymi środowiskami takimi jak Teams jest darmowa.

Cognitive Services – np usługa zmiany mowy w tekście.

Cognitive Services ma różne usługi. Np. Wspierające podejmowanie decyzji:

Anomaly detector- wykrywanie anomalii

Content Moderator – szuka w wypowiedziach brzydkie słowa

Personalizer – w oparciu o znajomość danych o użytkowniku próbuje dopasować wrażenia w nowych aplikacjach na takie, które użytkownik lubi

Dotyczące języka:

Immersion Reader – wspiera użytkowników mających problemy ze wzrokiem w czytaniu tekstów

Language Understanding – próbuje zrozumieć sens wypowiedzi

QnA Maker – odnajduje odpowiedź na pytanie z poli najczęściej zadawanych pytań

Text Analytics – szuka w tekście odpowiedzi czy dana wypowiedź jest ozytywna czy negatywna

Translator Text – służy do tłumaczenia tekstu

Speech Recognition – rozpoznawanie użytkownika w oparciu o głos

Usługi z gatunku vision:

Computer Vision – program opisuje co jest widoczne na obrazku

Custom Vision – w oparciu o zdjęcie produktu oceniamy jego jakość

Face recognition –

Form Recognizer-

Jest jeszcze zestaw usług służący do wyszukiwania danych oparty o bing.

### **Firewall i ochrona sieci przed DDoS**

Azure Firewall – zabezpiecza sieć w Azure. Zadaniem firewalla jest zezwolenie na taki ruch który świadomie dopuszczaemy. Określamy źródło ruchu (adres ip i numer portu) i cel ruchu (adres ip i port na który pakiet ma przyjść). Firewall Azure jest statefull – zachowuje w pamięci stan połączek. Pakiety już raz zaakceptowane w ramach połączenia już później będą akceptowane.

Oprócz określenia jaki ruch ma być z zewnątrz dopuszczony firewall określa też jaki ruch ma być dopuszczony z wewnątrz do internetu. Gdyby ktoś włamał się do nas i chciał wyprowadzić dane.

Azure Firewall dobrze się skaluje.

Reguły w firewallu mogą być następujących typów:

NAT – do firewalla dochodzą pakiety kierowane na zewnętrzny adres IP z różnego rodzaju numerami portów. Firewall decyduje, czy można przekazać pakiet do określonego adresu wewnętrznego na określony port. Pozwala to na konfigurowanie usług az firewallem, które będą dostępne z zewnątrz.

Zwykłe reguły które obowiązują wewnątrz firewalla – dopuszczały ruch z jednego punktu do innego punktu.

Reguły aplikacyjne – zezwalanie na połączenia w imieniu danej aplikacji.

Firewall patrzy nie tylko na reguły ale stosuje też machine learning.

Jak budujemy sieć w Azure? Buduje sieć, dzieli na posieci, przypisuję do sieci adres zewnętrzny i konfiguruje firewealla. Wewnętrznej podsieci z serwerami usług buduję sieć dla administratorów. Są one zwane JumpBox.

Innym rodzajem ataku przed jakim musi się bronić sieć to DDoS (Distributed Denial of Service). Dużo zainfekowanych stacji w jednym czasie nawiązuje połączenie z naszą siecią.

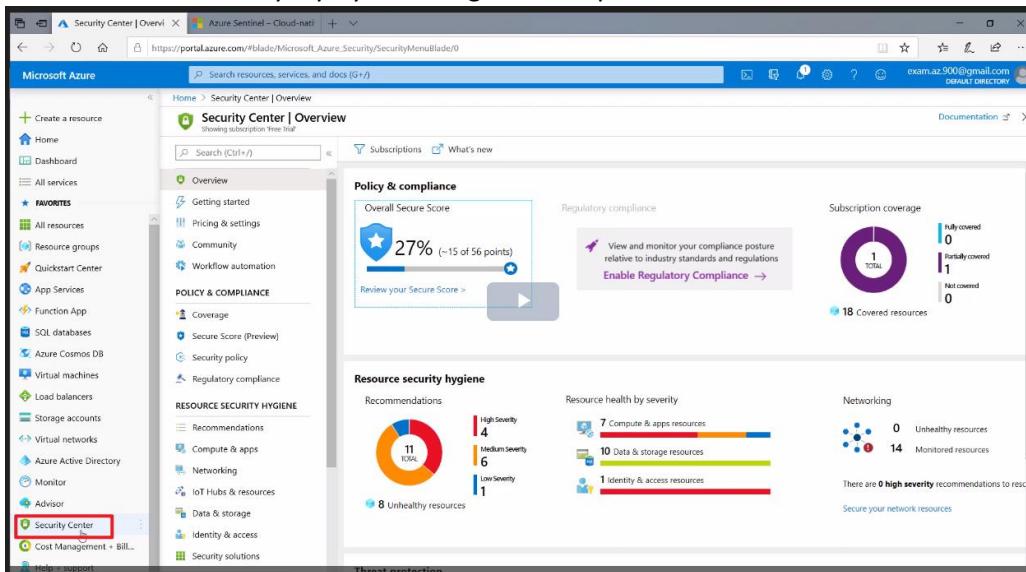
Azure DDoS Protection – mamy dwa plany:

1. Basic – zawsze przypisany do sieci wirtualnej w Azure. Nie loguje ataków i ich nie raportuje, nie tworzy alertów. Darmowy.
2. Standard – Loguje atak, alertuje o problemie i jest wsparcie od Microsoftu. Automatycznie skaluje w przypadku ataku. Odpłatny.

## Security Center, Sentinel, security portals

Security center – służy do monitorowania i zarządzania bezpieczeństwem. Są 2 plany:

1. Free – monitorowanie maszyn wirtualnych i aplikacji
2. Standard – dodatkowo monitorowanie bazy danych, storage i powala na uruchamianie zaawansowane metody wykrywania zagrożeń bezpieczeństwa



W sekcji getting started mamy propozycje zmian jakie możemy dokonać:

The screenshot shows the Azure Security Center Getting started page. The left sidebar has a 'Getting started' link highlighted with a red box. The main content area displays a summary of monitoring status: 'Enable standard tier on 1 subscription'. Below this is a table showing one subscription named 'Free Trial' with 16 total resources.

Name	Total resources
Free Trial	16

Coverage pozwala ustalić które subskrypcje są monitorowane.

Secure score – jakie zagrożenia zostały wykryte.

The screenshot shows the Azure Security Center Secure Score (Preview) page. The left sidebar has a 'Secure Score (Preview)' link highlighted with a red box. The main content area displays the 'Overall Secure Score' as 27% (~15 of 56 points). Below this is a table titled 'Subscriptions with the lowest scores' showing one entry for 'Free Trial' with a score of 27% (~15 of 56 points). A 'View recommendations >' button is highlighted with a red box at the bottom right of the table.

Subscription	Secure Score
Free Trial	★ 27% (15 of 56)

Mamy tutaj propozycje, które mają zwiększyć bezpieczeństwo:

Controls	Potential score increase	Unhealthy resources	Resource Health
> Enable MFA	+ 18% (10 points)	1 of 1 resources	<div style="width: 10%; background-color: red;"></div>
> Apply system updates	+ 11% (6 points)	4 of 4 resources	<div style="width: 25%; background-color: red;"></div>
> Remediate vulnerabilities	+ 11% (6 points)	4 of 4 resources	<div style="width: 25%; background-color: red;"></div>
> Enable encryption at rest	+ 7% (4 points)	4 of 4 resources	<div style="width: 25%; background-color: red;"></div>
> Manage access and permissions	+ 7% (4 points)	1 of 1 resources	<div style="width: 10%; background-color: red;"></div>
> Remediate security configurations	+ 7% (4 points)	4 of 4 resources	<div style="width: 25%; background-color: red;"></div>
> Apply adaptive application control	+ 5% (3 points)	4 of 4 resources	<div style="width: 25%; background-color: red;"></div>
> Enable endpoint protection	+ 4% (2 points)	4 of 4 resources	<div style="width: 25%; background-color: red;"></div>
> Enable auditing and logging	+ 2% (1 point)	1 of 1 resources	<div style="width: 10%; background-color: red;"></div>
> Encrypt data in transit	+ 1% (1 point)	2 of 12 resources	<div style="width: 16%; background-color: yellow;"></div>
> Implement security best practices	+ 0% (0 points)	4 of 22 resources	<div style="width: 10%; background-color: red;"></div>
> Protect applications against DDoS attacks	+ 0% (0 points)	None	<div style="width: 0%; background-color: grey;"></div>

Możemy sprawdzić czy moja organizacja spełnia określone normy prawne określane jako compliance:

What is Regulatory Compliance?

Regulatory Compliance enables you to monitor your environment for risks based on compliance standards, and view a report that shows your compliance posture relative to each standard. You can filter by regulations, export reports, and resolve compliance issues directly within the experience.

How does it work?

Security Center assessments have been mapped to compliance regulations, such that each applicable regulation control has some assessments associated with it. You can view your compliance relative to the supported controls of a regulation based on the passing vs. failing assessments that align with that regulation. As you remediate more assessments, your compliance posture improves.

Microsoft zapewnia na stronie raporty z audytów i dowody na spełnienie compliance – ta strona to trust center

Strona service trust pozwala przejrzeć wyniki audytów microsoftu

Jest jeszcze compliance manager – tam są akty prawne jakie odtyczają mojej firmy. Jeśli muszę wykazać zgodność z tymi normami możemy otworzyć formularz i zapoznać się za co odpowiada microsoft a za co ja

Azure Sentinel – to implementacja Security Information and Event Management. W usłudze tej informacje które ciągle napływają mogą być przetworzone w sprytny sposób. Dane, które zostały zebrane są analizowane i wykrywane jest spośród wielu możliwych prób ataku te zdarzenia, które potwierdzają, że rzeczywiście jest atak i w tym przypadku wygenerować incydent i automatycznie rozwiązać problem zamkając port albo blokując konto użytkownika zainfekowanego.

Na egzamienie pytania o:

Trust Center - podstawowe informacje o tym jak Microsoft implementuje bezpieczeństwo

Compliance Manager - narzędzie do budowania własnych dokumentów compliance w oparciu o compliance Microsoft

Service Trust - wyniki audytowe Microsoft

to prawie pewniaki! Dlatego postaraj się zapamiętać, którego narzędzia kiedy użyć.

Przejrzyj poniższe strony, żeby utrważyć sobie znaczenie poszczególnych stron:

Trust Center <https://www.microsoft.com/en-ww/trust-center>

Compliance Manger <https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide>

Service Trust <https://servicetrust.microsoft.com/>

## Key Vault

Key Vault – pozwala na przechowywanie haseł, kluczy, sekretów, certyfikatów w bezpieczny sposób w Azure. Żeby mieć do nich dostęp trzeba mieć uprawnienia a te przyznaje się w oparciu o Active Directory.

Mamy 2 plany Key Vault – standard i premium. Obydwa są płatne. W przypadku premium można korzystać z informacji kodowanej w hardware secret modules.

Nazwa Key Vault musi być unikalna.

Tworzymy Key Vault:

The screenshot shows the 'Create key vault' wizard in the Azure portal. The current step is 'Access policy'. It lists users and their access rights. The user 'Exam AZ-900' is selected with the following permissions:

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
USER	Exam AZ-900	9 selected	7 selected	15 selected	Delete

W zakładce policy określamy kto będzie miał prawo do zarządzania wbudowanym Key Vault. Networking określa z jakiej sieci można łączyć się do KV.

Miejsca gdzie wprowadzamy to pozycje Keys, Secrets i Certificates:

The screenshot shows the 'Access policies' section of the Azure Key Vault 'CityDev-KV'. The left sidebar lists various management options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events (preview), Settings, Keys, Secrets, Certificates, and Access policies. The 'Access policies' option is currently selected and highlighted in grey. Under 'Access policies', there are sub-options: Networking, Properties, Locks, and Export template.

W Access policies zarządzamy uprawnieniami do czytania sekretów.

Sieciami zarządzamy w networking.

Dodaliśmy nowy secret. Modyfikacje secretu robi się tak, że dodaje się nową wersję:

The screenshot shows the 'db-password' secrets list in the Azure Key Vault 'CityDev-KV'. At the top, there is a 'New Version' button. Below it, there is a table with two rows. The first row is labeled 'CURRENT VERSION' and contains the version '95e6d3b49229473da60fbab1d6a84a64' and status 'Enabled'. The second row contains a plus sign icon and the text 'New Version'.

Version	Status	Activation Date	Exp
95e6d3b49229473da60fbab1d6a84a64	✓ Enabled		

Stara wersja nadal będzie osiągalna.

W Logic App zrobimy prostą aplikację, której jedynym zadaniem będzie odczyt klucza.

https://portal.azure.com/#create/MicrosoftEmptyWorkflow

**Basics \* Review + create**

**Project details**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

**Subscription \*** Free Trial  
**Resource group \*** KeyVault-RG [Create new](#)

**Instance details**  
**Logic App name \*** KeyValue-GetKey  
**Select the location**  Region  Integration Service Environment  
**Location \*** (US) East US  
**Log Analytics**  On  Off

[Review + create](#) [Download a template for automation](#)

### Nasza aplikacja ma być uruchamiana przez link URL:

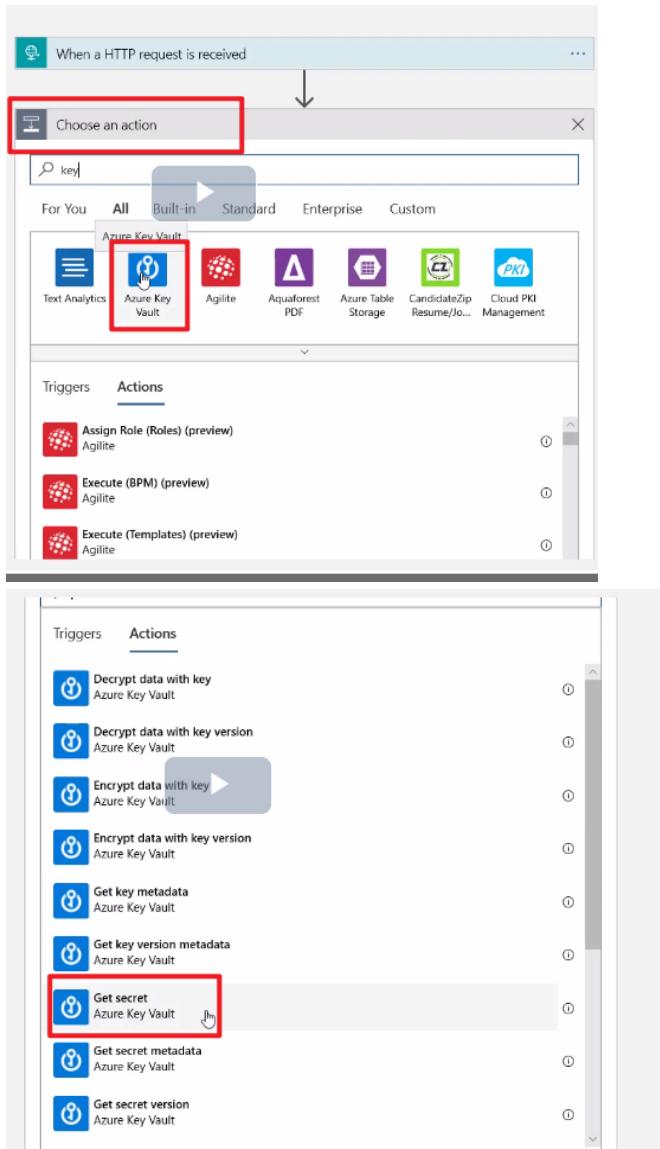
Introducing Azure Logic Apps [Watch later](#) [Share](#)

Building integration solutions is easier than ever. Logic Apps brings speed and scalability into the enterprise integration space. The ease of use of the designer, variety of available triggers and actions, and powerful management tools make centralizing your APIs simpler than ever. As businesses move towards digitalization, Logic Apps allows you to connect legacy and cutting-edge systems together.

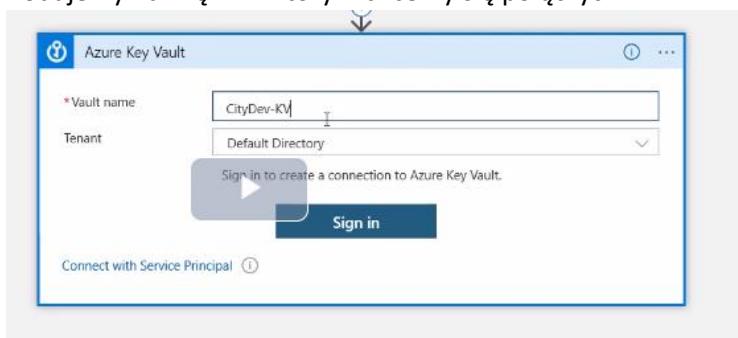
- Create business processes and workflows visually
- Integrate with SaaS and enterprise applications
- Unlock value from on-premises and cloud applications

Start with a common trigger  
Pick from one of the most commonly used triggers, then orchestrate any number of actions using the rich collection of connectors

	When a message is received in a Service Bus queue		When a HTTP request is received		When a new tweet is posted		When an Event Grid resource event occurs
	Recurrence		When a new email is received in Outlook.com		When a new file is created on OneDrive		When a file is added to FTP server



Podajemy nazwę KV z którym chcemy się połączyć:



Wskazujemy które hasło ma być pobrane:



Odpalamy i widzimy wyniki:

Akcja została wykonana na moich credentialach więc to tak jakbym ja odczytywał hasło. Jeśli miałyby to się odbywać na credentialach aplikacji to trzeba to zrobić nieco inaczej. Wracamy do Logic app:

Obecnie aplikacja działa na moich credentialach. Jeśli chcę to zmienić to w System assigned zmieniamy status na on:

The screenshot shows the 'Identity' section of an Azure Logic App named 'KeyVault-GetKey'. The 'System assigned' identity is enabled. A status switch is set to 'On'. There are buttons for 'Save', 'Discard', 'Refresh', and 'Got feedback?'

Od tej pory apka działa na specjalnym nowym koncie. Trzeba je skonfigurować. Przechodzimy do naszego Key Vault i do Access Policies:

The screenshot shows the 'Overview' page of a Key Vault named 'CityDev-KV'. The 'Access policies' option in the left sidebar is highlighted with a red box. The main pane displays vault details like Resource group, Location, Subscription, and DNS Name.

Tutaj wskazujemy kto ma dostęp do tego klucza:

The screenshot shows the 'Access policies' page of the 'CityDev-KV' Key Vault. The '+ Add Access Policy' button in the top-left is highlighted with a red box. A table lists existing access policies for a user named 'Exam AZ-900'.

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
Exam AZ-900	exam.az_900_gmail.co...	9 selected	7 selected	15 selected	Delete

The screenshot shows the 'Add access policy' screen in the Azure portal. At the top, there's a breadcrumb navigation: Home > Resource groups > KeyVault-RG > CityDev-KV | Access policies > Add access policy. Below this, the title 'Add access policy' is followed by a sub-section 'Add access policy'. A dropdown menu titled 'Configure from template (optional)' is expanded, listing several management categories. The 'Secret Management' category is specifically highlighted with a red box.

Wskazujemy komu chcemy nadać uprawnienia:

The screenshot shows the 'Add access policy' screen in the Azure portal. The 'Principal' section is active, showing a search interface for selecting a principal. The search bar contains the text 'Key'. A result named 'KeyVault-GetKey' is listed and highlighted with a red box. On the left side of the screen, there are sections for 'Key permissions' (0 selected), 'Secret permissions' (7 selected), and 'Certificate permissions' (0 selected). The 'Certificate permissions' section is also highlighted with a red box.

Za pomocą audytu można śledzić kto korzysta z klucza.

## Coś dla architektów – Blueprint

Azure Blueprint – ma wspomóc architektów pracujących na rzecz wielkiej organizacji. Wcześniej omawialiśmy szablony ARM – wyklikaliśmy obiekt w interfejsie a później eksportowaliśmy template i tworzyliśmy na tej postawie kolejne obiekty.

Blueprint to pojemnik z wieloma szablonami ARM, definicjami grup zasobów i wiele więcej. Raz powstały blueprint możemy później wdrażać. Dzięki temu kolejne powstałe aplikacje będą podobne.

Mamy resource grupę z Key Vaultem i Virtual network w środku:

The screenshot shows the Azure portal interface for a resource group named 'Master101'. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Events, Settings, Quickstart, Deployments, Policies, Properties, and Locks. The main area displays the 'Overview' tab for the resource group. It includes details such as Subscription (change) : Free Trial, Subscription ID : 08d2a365-709d-48b2-8fb4-7073703f4ec7, and Tags (change) : Click here to add tags. Below this, a table lists resources: 'Name ↑' and 'Type ↑↓'. Two resources are listed: 'Master101-KV' (Key vault) and 'Master101-VNET' (Virtual network). Both of these entries are highlighted with a red box.

Przypuśćmy, że jest to szablon aplikacji na podstawie którego będziemy tworzyć inne aplikacje. Wyeksportujemy zasoby ARM poszczególnych zasobów. Wchodzimy w pierwszy z nich –Key vault i idziemy do export template:

The screenshot shows the Azure portal interface for a key vault named 'Master101-KV'. The left sidebar includes Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events (preview), Settings (with sub-options Keys, Secrets, Certificates, Access policies, Networking, Properties, Locks), Monitoring, and a 'More' section. In the 'Settings' menu, the 'Export template' option is highlighted with a red box. The main area shows a summary with a warning icon: 'Resc', 'Loca', 'Sub:', 'Sub:', 'Mor', 'Short', '1 Click', and 'Tot'.

Zapisujemy w pliku wygenerowany tekst albo klikamy download:

The screenshot shows the Azure Resource Manager blade. On the left, there's a sidebar with navigation links like Overview, Activity log, Tags, Diagnose and solve problems, and Settings (Address space, Connected devices, Subnets, DDoS protection, Firewall, Security, DNS servers, Peerings, Service endpoints, Private endpoints, Properties). The main area has tabs for Template, Parameters, and Scripts. The Template tab is selected and displays a JSON deployment template. A red box highlights the JSON code. At the top of the main area, there are buttons for Download, Add to library (preview), and Deploy. A note says "To export related resources, select the resources from the Resource Group view then select the "Export template" option from the tool bar." There's also a checked checkbox for "Include parameters".

```
1 {
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "virtualNetworks_Master101_VNET_name": {
      "defaultValue": "Master101-VNET",
      "type": "String"
    }
  },
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Network/virtualNetworks",
      "apiVersion": "2019-12-01",
      "name": "[parameters('virtualNetworks_Master101_VNET_name')]",
      "location": "centralus",
      "tags": {
        "TEMPLATE": "MASTER_BP"
      },
      "properties": {
        "addressSpace": {

```

Przechodzimy do Policy i Blueprints:

The screenshot shows the Azure Policy Overview page. The top navigation bar includes a search bar, a user icon, and the URL exam.az.900@gmail.com DEFAULT DIRECTORY. The main content area has a title 'Policy' and a sidebar with sections like Overview, Getting started, Join Preview, Compliance, Remediation, Authoring, Assignments, Definitions, and Related Services (Blueprints (preview) is highlighted with a red box). Key metrics displayed are Overall resource compliance at 91% (179 out of 197), Non-compliant initiatives at 1 (out of 1), Non-compliant policies at 38 (out of 99), and Non-compliant resources at 18 (out of 197). A video player is present below the metrics. On the right, there's a 'LEARN MORE' section with links to 'Learn about Policy' and 'Onboarding tutorial'. A table lists assignments by compliance status.

The screenshot shows the Azure Blueprints | Getting started page. The top navigation bar includes a search bar, a user icon, and the URL exam.az.900@gmail.com DEFAULT DIRECTORY. The main content area has a title 'Blueprints | Getting started' and a sidebar with sections like Getting started, Blueprint definitions, and Assigned blueprints. A central diagram illustrates the blueprint creation process. Below it, three main actions are listed: 'Create a blueprint' (button highlighted with a red box), 'Apply to a scope', and 'Track'. A 'Welcome to Azure' section provides an overview of what blueprints are and how to get started.

Mamy różne szablony ale my tworzymy blueprint od zera:

The screenshot shows the 'Create blueprint' page in the Azure portal. At the top, there's a breadcrumb navigation: Home > Policy > Blueprints | Getting started > Create blueprint. The main heading is 'Create blueprint'. Below it, a section titled 'Choose a blueprint sample' says: 'You can start with a blank blueprint or pick one of our pre-defined samples to help you get started quickly'. There's a 'Blank Blueprint' card with a small icon, a description: 'An empty blueprint with no initial properties or artifacts.', and a blue button labeled 'Start with blank blueprint' which is highlighted with a red box. To the right of the card is a play button icon. Below this section is a heading 'Other Samples' with a search bar. A table lists several samples:

Name	Description
Azure Security Benchmark	Assigns policies to address specific recommendations from the Azure Security Benchmark. <a href="#">Learn more</a>
Basic Networking (VNET)	Configures a virtual network with a subnet and an NSG.
CAF Foundation	Microsoft Cloud Adoption Framework for Azure – Configure Foundational best practices <a href="#">Learn more</a>
CAF Migration landing zone	Microsoft Cloud Adoption Framework for Azure – Migrations landing zone <a href="#">Learn more</a>
Canada Federal PBMM	Assigns policies to address Canada Federal PBMM controls. <a href="#">Learn more</a>

Blueprint można grupować w management grupy. I właśnie w management grupie można zapisać blueprinta:

The screenshot shows the 'Create blueprint' page in the Azure portal. The 'Definition location' section is highlighted with a red box. It contains fields for 'Management Group' (set to 'Tenant Root Group') and 'Subscription' (set to 'Optional choose a Subscription'). Below these fields is a note: 'The management group or subscription where the blueprint is saved. The definition location determines the scope that the blueprint may be assigned to. Learn more at [aka.ms/BlueLocation](#)'.

Określamy co ma być w blueprincie:

The screenshot shows the 'Create blueprint' page with the 'Artifacts' tab selected. The 'Add artifact...' button is highlighted with a red box. On the right, a modal window titled 'Add artifact' shows a list of artifact types: 'Policy assignment', 'Role assignment', 'Azure Resource Manager template (Subscription)', and 'Resource group'. 'Resource group' is also highlighted with a red box.

Mögemy na stałe ustalić jaka będzie nazwa tej resource grupy z blueprinta. Ale mögemy określić, że będzie to parametr i użytkownik za każdym razem będzie pytany jak grupa zasobów ma się nazywać:

The screenshot shows the 'Add artifact' configuration window. The 'Artifact type' is set to 'Resource group'. The 'Artifact display name' is 'AppRG'. A note says: 'You can choose to fill these parameters in now or when assigning the blueprint.' The 'Resource Group Name' field is empty. A checkbox 'This value should be specified when the blueprint is assigned' is checked and highlighted with a red box. The 'Location' is set to 'East US'. Another checkbox 'This value should be specified when the blueprint is assigned' is checked below it. At the bottom, there's a section for 'Resource Group Tags (Optional)' with a table for 'Tag Name' and 'Tag Value'.

Dodajemy kolejne zasoby. Mamy już dwa miejsca do dodawania:

The screenshot shows the 'Create blueprint' interface. Under the 'Artifacts' tab, there are two sections for adding artifacts: 'Subscription' and 'AppRG'. Each section has a red box around the '+ Add artifact...' button.

Do tej resource grupy dodajemy VNET:

The screenshot shows the 'Create blueprint' interface with the 'Artifacts' tab selected. A modal window titled 'Add artifact' is open, showing a dropdown menu for 'Artifact type \*'. The 'Azure Resource Manager template' option is highlighted with a red box.

Wskazujemy templatkę:

The screenshot shows the 'Add artifact' modal with the 'Template' tab selected. It includes fields for 'Artifact type \*' (set to 'Azure Resource Manager template'), 'Artifact display name \*' (set to 'VNET'), and a 'Description' text area. At the bottom, the 'Template' tab is selected, and a red box highlights the 'Import template' section, which contains a file input field and a preview area showing '1 [ ]'.

Analogicznie dodajemy Key Vault.

Drafty blueprinta są tutaj:

The screenshot shows the 'Blueprints | Blueprint definitions' page in the Azure portal. A red box highlights the 'Blueprint definitions' link in the left sidebar. The main area displays a table with one row for 'KVApplication-BP'. The row details are: Name: KVApplication-BP, Latest Version: Draft, Unpublished ch...: Yes, Last modified: 4/30/2020, Definition location: Free Trial. A large play button icon is overlaid on the table.

Jak blueprint jest gotowy to go publikujemy:

The screenshot shows the 'KV Application-BP Blueprint' details page. A red box highlights the 'Publish Blueprint' button. Below it, the blueprint information is listed: Name: KVApplication-BP, State: Draft, Definition location: Free Trial, Definition location ID: 08d2a365-709d-48b2-8fb4-7073703f4ec7, Version: Draft. The 'Latest artifacts' section lists four artifacts: Assigned subscription (Subscription), AppRG (Resource group), VNET (Azure Resource Manager template), and KV (Azure Resource Manager template). A play button icon is overlaid on the artifacts table.

Przygotowany blueprint implementujemy na subskrypcji:

The screenshot shows the 'KVApplication-BP Blueprint' details page again. A red box highlights the 'Assign Blueprint' button. The blueprint information is identical to the previous screenshot. The 'Latest artifacts' section also remains the same, listing the four artifacts. A play button icon is overlaid on the artifacts table.

Mozemy zakładać blokadę żeby nikt nie mógł blokować lub usuwać zasobów:

Search resources, services, and docs (G+/J)

Home > Policy > Blueprints | Blueprint definitions > KVApplication-BP > Assign blueprint

### Assign blueprint

Blueprint definition version \* ⓘ  
1.0

Lock Assignment  
Don't Lock (selected) Do Not Delete Read Only

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources.  
Learn more

Managed Identity ⓘ  
System assigned (selected)  
User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all Artifacts. We will automatically remove this access when the blueprint assignment process is finished.

Artifact parameters

Artifact / Parameter	Parameter Value
Subscription	

Assign Cancel

Określamy jak mają się nazywać komponenty blueprinta:

Search resources, services, and docs (G+/J)

Home > Policy > Blueprints | Blueprint definitions > KVApplication-BP > Assign blueprint

### Assign blueprint

System assigned (selected)  
User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all Artifacts. We will automatically remove this access when the blueprint assignment process is finished.

Artifact parameters

Artifact / Parameter	Parameter Value
Subscription	KVApp01
AppRG	Resource Group: Name: KVApp01 Resource Group: Location: westus2
KV	vaults_Master101_KV_name (KV): App01-KV
VNET	virtualNetworks_Master101_VNET_name (VNET): App01-VNET

Assign Cancel

Sprawdzamy czy instalacja blueprinta powiodła się:

Home > Policy > Blueprints | Assigned blueprints

## Blueprints | Assigned blueprints

Search (Ctrl+/) Refresh

Subscriptions: Free Trial

Assignment name	Subscription	Blueprint	Version	Provisioning state	Date assigned	...
Assignment-KVApplication-BP	Free Trial	KVApplication-BP	1.0	Succeeded	4/30/2020	...

Architekt albo zespół który wymyśla szablony może zamiast przekazywać zespołowi deweloperów dokument mówiący o tym jak budować aplikacje może przekazać gotowy blueprint. Zespół deweloperów wdroży go na swojej subskrypcji.

## Konfiguracja monitoringu i alertów

Żeby aplikacja była śledzona trzeba włączyć dla niej monitoriing. Włączamy monitoring. Podczas wykonywania tej czynności serwer musi działać. Przechodzimy do maszyny wirtualnej i do sekcji Insights:

Home > Virtual machines > srv01

Search resources, services, and docs (G+)

srv01  
Virtual machine

Inventory

Change tracking

Configuration management ...

Policies

Run command

**Monitoring**

- Insights**
- Alerts
- Metrics
- Diagnostic settings
- Advisor recommendations
- Logs
- Connection monitor

Support + troubleshooting

- Resource health
- Boot diagnostics
- Performance diagnostics (Pr...)
- Reset password
- Redeploy

Connect Start Restart

Advisor (1 of 4): Monitoring agent health issue

Resource group (change) : RestrictedRG

Status	: Running
Location	: East US
Subscription (change)	: Free Trial
Subscription ID	: 08d2a365-709d-48
Computer name	: srv01
Operating system	: Linux (ubuntu 18.0
Size	: Standard B1ms (1 v
Tags (change)	: Click here to add ta

Show data for last:

CPU (average)

100%

80%

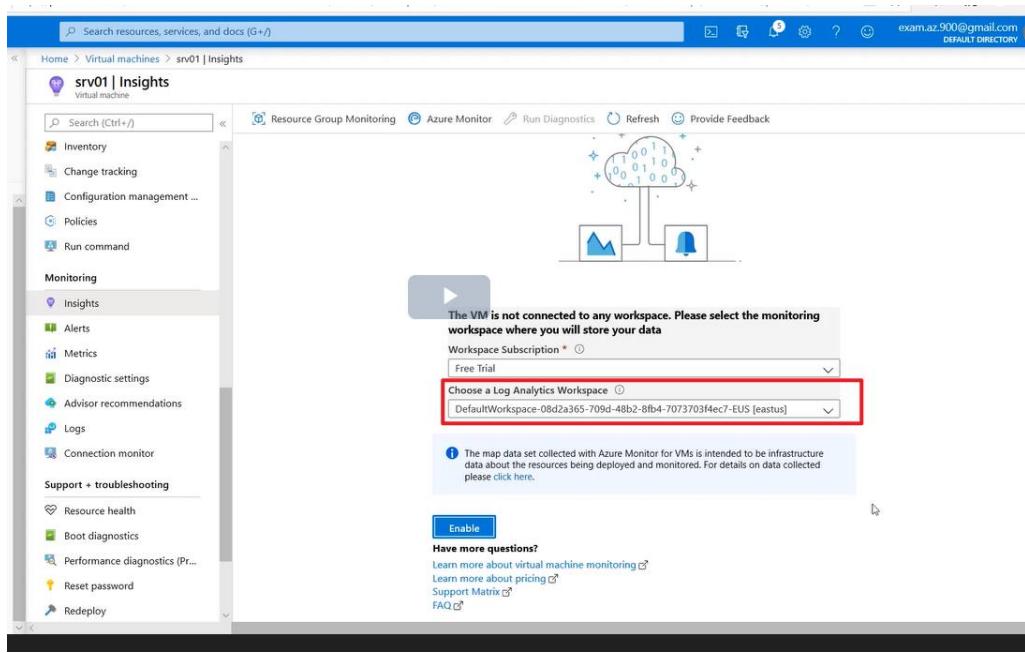
60%

40%

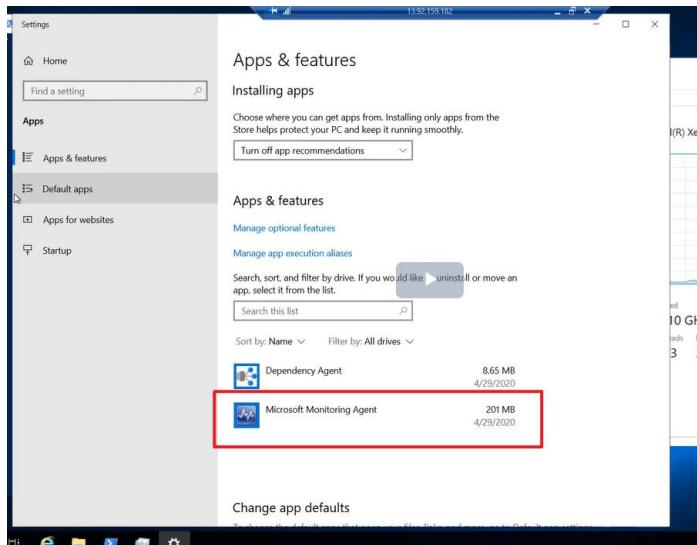
20%

e4860-6617-4def-ac43-f80209197327/resource/subscriptions/08d2a365-709d-48fb4-7073703f4ec7/resource

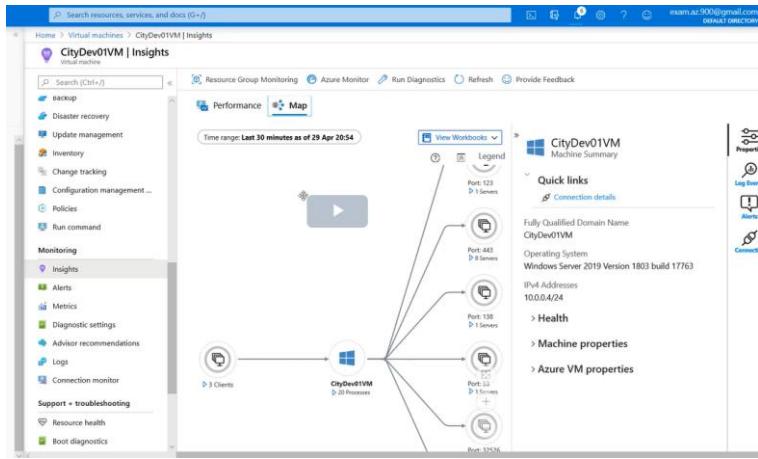
Informacje o monitoringu muszą być przechowywane. I dlatego jest Log Analytics Workspace:



Jeśli włączyliśmy monitoringu dla maszyny windowsowej to po wejściu do tej maszyny widzimy, że pojawił się Microsoft Monitoring Agent:



Jak wróćmy do sekcji Insights to teraz wygląda ona tak:



W przypadku gdybyśmy chcieli być informowane o problemach trzeba skonfigurować alert, który będzie sam się wzbudzał gdy dojdzie do niepoprawnej sytuacji na serwerze. Definiujemy regułę:

Severity	Total Alerts	New	Acknowledged	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0
Sev 2	0	0	0	0
Sev 3	1	1	0	1
Sev 4	0	0	0	0

Musimy podać 3 rzeczy: jaki zasób ma podlegać alertowaniu, warunek : weźmiemy przeciążenie CPU:

Configure signal logic

Choose a signal below and configure the logic on the next screen to define the alert condition.

Signal type: All | Monitor service: All

Displaying 1 - 20 signals out of total 50 signals

Signal name	Signal type	Monitor service
Percentage CPU	Metric	Platform
Network In Billoable (Deprecated)	Metric	Platform
Network Out Billoable (Deprecated)	Metric	Platform
Disk Read Bytes	Metric	Platform
Disk Write Bytes	Metric	Platform
Disk Read Operations/Sec	Metric	Platform
Disk Write Operations/Sec	Metric	Platform
CPU Credits Remaining	Metric	Platform
CPU Credits Consumed	Metric	Platform
Data Disk Read Bytes/Sec (Deprecated)	Metric	Platform
Data Disk Write Bytes/Sec (Deprecated)	Metric	Platform
Data Disk Read Operations/Sec (Deprecated)	Metric	Platform
Data Disk Write Operations/Sec (Deprecated)	Metric	Platform
Data Disk QD (Deprecated)	Metric	Platform

Ustawiamy, że wzbudzenie ma nastąpić gdy średnie wykorzystanie CPU będzie wynosiło powyżej 60% przez 5 minut z próbkowaniem co minute:

Configure signal logic

Alert log: Percentage CPU (Avg) 30.72 %

Threshold: Static

Operator: Greater than

Aggregation type: Average

Threshold value: 60 %

Condition preview: Whenever the percentage cpu is greaterthan 60 %

Evaluated based on: Aggregation granularity (Period): 5 minutes, Frequency of evaluation: Every 1 Minute

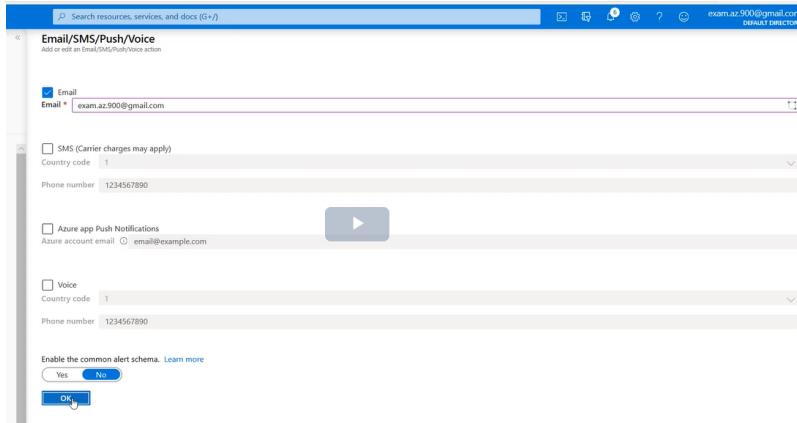
Ostatnia rzecz jaką ustawiamy – jaka ma być odpowiedź na ten alert:

The screenshot shows the 'Create rule' page in the Azure portal. At the top, there's a search bar and a breadcrumb navigation path: Home > Virtual machines > CityDev01VM | Alerts > Create rule. The main area is titled 'Create rule' under 'Rules Management'. A 'HIERARCHY' section shows 'CityDev01VM' as the resource. Below it, a 'CONDITION' section is set to 'Monthly cost in USD (Estimated)' with a value of '\$ 0.10'. An 'Add' button is available to add more conditions. A red box highlights the 'ACTIONS GROUPS (optional)' section, which contains an 'Action group name' field ('Contain actions') and an 'Add' button. A note below says: 'Action rules (preview) allows you to define actions at scale as well as suppress actions. Learn more about this functionality by clicking on this banner.' A 'Create alert rule' button is at the bottom.

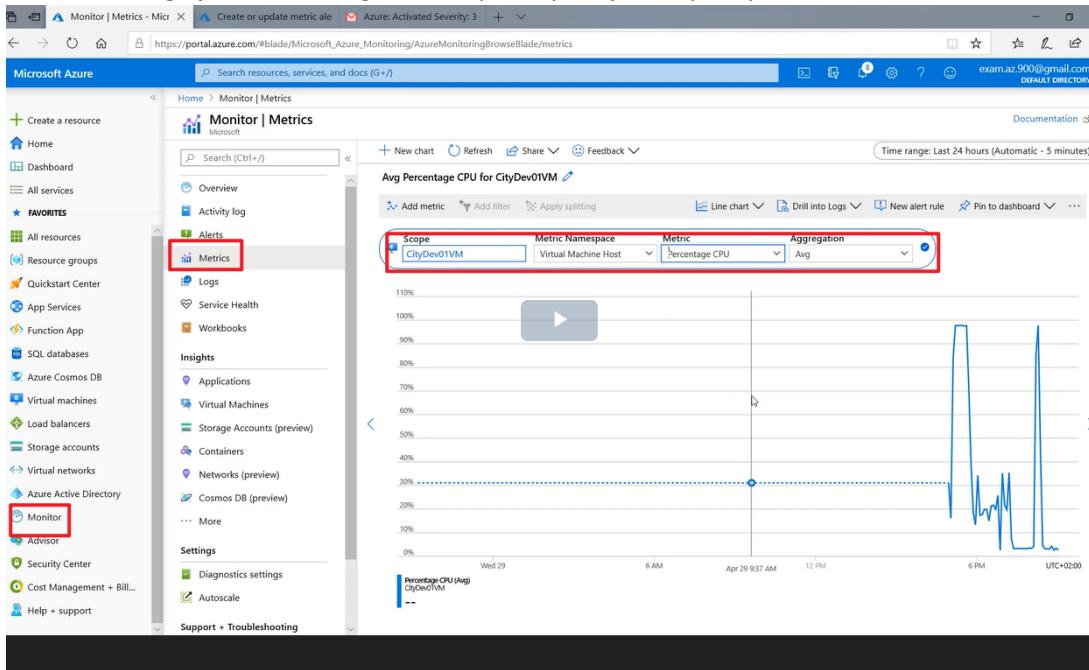
Mozemy tu stworzyć albo wybrać akcję jaka ma się wydarzyć. Stworzymy maila do admina:

The screenshot shows the 'Add action group' dialog. It includes fields for 'Action group name' (Email to administrator), 'Short name' (EmailAdmin), 'Subscription' (Free Trial), and 'Resource group' (Default-ActivityLogAlerts). A 'Actions' section shows an 'Action name' (EmailAdmin) and a dropdown menu for 'Action Type' with options like 'Select an action type', 'Automation Runbook', 'Azure Function', etc. A note says: 'Have a consistent details. Click on the Privacy Statement or Pricing link.' A 'OK' button is at the bottom right.

Wybieramy email/sms/push/voice i wskazujemy adres:



Jest cos takiego jak monitoring. Możemy tam podejrzeć np. użycie CPU:



## Azure Advisor

Azure Advisor zawiera sugestie, które pozwolą poprawić jakość korzystania z chmury. W sekcji overview można sprawdzić co da się w subskrypcji poprawić. Analizie poddane są takie elementy jak:

- cost
- security
- high availability
- operational excellence
- performance

The screenshot shows the Azure Advisor blade with the following details:

- Subscriptions:** Free Trial
- Cost:** 11 Recommendations (2 High impact, 7 Medium impact, 2 Low impact), 8 Impacted resources.
- Security:** 2 Recommendations (0 High impact, 2 Medium impact, 0 Low impact).
- High Availability:** 2 Recommendations (0 High impact, 2 Medium impact, 0 Low impact).
- Operational Excellence:** 1 Recommendation (0 High impact, 1 Medium impact, 0 Low impact).
- Performance:** No recommendations shown.

Azure sugeruje korzystanie z backupów:

The screenshot shows the Azure Advisor | High Availability blade with the following details:

- Subscriptions:** Free Trial
- Total recommendations:** 2
- Recommendations by impact:** 0 High impact, 2 Medium impact, 0 Low impact.
- Impacted resources:** 4
- Impact and Description:**

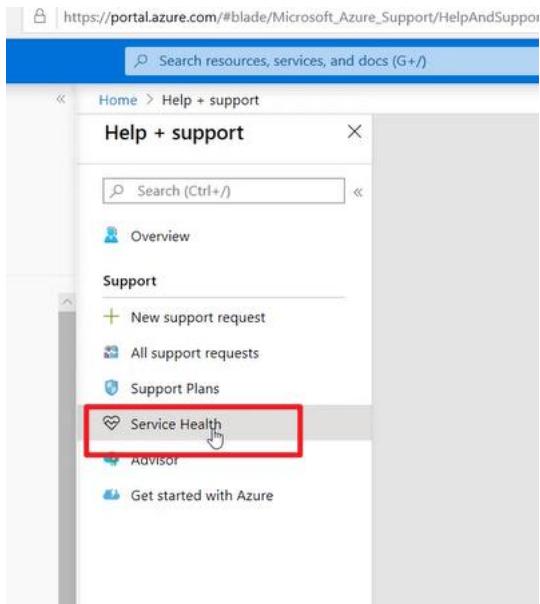
IMPACT	DESCRIPTION
Medium	Enable virtual machine backup to protect your data from corruption and accidental deletion
Medium	Enable Soft Delete to protect your blob data
- Potential Benefits:**
  - Improved data resilience and performance (1 Virtual machine, 4/29/2020, 10:18:30 PM)
  - Save and recover your data when blobs or blob snapshots are accidentally overwritten or deleted (3 Storage Accounts, 4/29/2020, 6:35:04 PM)

Informację o stanie zdrowia Azure można uzyskać w sekcji help and support:

The screenshot shows the Microsoft Azure blade with the following details:

- Create an Azure service health alert:**
  - Recommendation details:** Service health alerts help you stay notified when Azure service issues affect you. Create a service health alert for the regions and services that you care about. [Learn more](#)
  - Impacted resources:** Active (1) Postponed & Dismissed (0)
  - Actions:** SELECT SUBSCRIPTION (Free Trial) RECOMMENDED ACTIONS (Create an Azure service health alert)
- Help sidebar:**
  - Help + support:** Visit the help and support center to create or track a support ticket and monitor health.
  - What's new:** Azure roadmap, Launch guided tour, Keyboard shortcuts, Show diagnostics, Privacy statements.
  - Work with an expert:** Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. Find an Azure expert.

W Service Health można sprawdzić jakie prace są wykonywane albo do jakich incydentów doszło:



## Azure Active Directory

Centralnym miejscem do zarządzania tożsamością jest Azure Active Directory:

A screenshot of the Microsoft Azure dashboard. On the left, there's a sidebar with various service icons and links like Create a resource, Home, Dashboard, All services, FAVORITES (All resources, Resource groups, Quickstart Center, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Monitor, Advisor, Security Center, Cost Management + Bill..., and Help + support). The 'Virtual networks' link is highlighted with a red box. On the right, there's a 'Create a resource' button and icons for App Services, Azure Active Directory, and Security Center. Below that is a 'Recent resources' section with a list of items: CityinfoApp, Free Trial, teststorage303, and CityDev. A detailed view of the 'Azure Active Directory' service is shown, featuring a summary card with a blue triangle icon, a 'View' button, and a 'Free training from Microsoft' section about securing applications using OpenID Connect. There are also 'Useful links' for Overview, Get Started, and Pricing.

Użytkownicy mogą tu być zdefiniowani nie tylko w ramach subskrypcji ale możemy też dołączać użytkowników klientów, w oparciu o uwierzytelnienie w innych portalach.

Tworzymy konto dla nowego usera:

https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/ActiveDirectoryMe

The screenshot shows the 'Default Directory | Overview' page in the Azure portal. The left sidebar under 'Manage' has 'Users' selected and highlighted with a red box. Other options include Groups, Organizational relationships, Roles and administrators, Administrative units (Preview), Enterprise applications, Devices, and App registrations.

https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/UsersManagementMenuBlade/AllUsers

The screenshot shows the 'Users | All users (Preview)' blade. The top navigation bar includes 'Home > Default Directory > Users | All users (Preview)'. The '+ New user' button is highlighted with a red box. The main table displays two users: 'Exam AZ-900' and 'Peter Blue'.

https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/UsersManagementMenuBlade/AllUsers

The screenshot shows the 'Users | All users (Preview)' blade. The '+ New user' button is visible at the top. The main table displays two users: 'Exam AZ-900' and 'Peter Blue'. The 'Peter Blue' row is highlighted with a red box.

Możemy tworzyć użytkowników w sposób automatyczny:

Home > Default Directory > Users | All users (Preview)

**Users | All users (Preview)**

All users (Preview) Deleted users Password reset User settings Diagnose and solve problems

+ New user + New guest user Bulk create Bulk invite Bulk delete Download

Search users Add filters

Name	User name	User type
EA Exam AZ-900	exam.az.900@gmail.com	Member
PB Peter Blue	peter@examaz900gmail.onmicrosoft.c...	Member

Usuniętych użytkowników możemy odzyskać do 30 dni:

Home > Default Directory > Users | Deleted users

**Users | Deleted users**

All users (Preview) Deleted users Password reset User settings Diagnose and solve problems

Delete permanently Restore user Bulk restore Refresh Columns Got feedback?

Users are permanently deleted automatically 30 days after they are deleted.

Name	User name	User type	Source	Deletion date	Permanent deletion date
Chris Green	chrис@examaz900gma...	Member	Azure Active Directory	4/30/2020, 8:49:25 AM	5/30/2020, 8:49:25 AM

Mogliśmy tworzyć użytkowników i przypisywać im uprawnienia ale efektywniej jest tworzyć grupy i przypisywać tym grupom uprawnienia. Tworzymy grupę:

https://portal.azure.com/#blade/Microsoft\_AAD\_JAM/ActiveDirectoryMenuBlade/Overview

Home > Default Directory | Overview

**Default Directory | Overview**

Search (Ctrl+ /) Switch directory Delete directory + Create a directory What's new Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. Learn more

Overview

**Default Directory**

examaz900@gmail.onmicrosoft.com Tenant ID: 6e0e4860-6617-4def-a43-f80209197327 Azure AD Free

Manage

- Users
- Groups**
- Organizational relationships
- Roles and administrators (Pr...)
- Administrative units (Preview)
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses

Azure AD Connect

Status: Not enabled

Last sync: Sync has never run

Sign-ins

Są dwa rodzaje grup: Security i Office365:

Search resources, services, and docs (G+/)

Home > Default Directory > Groups | All groups > New Group

### New Group

**Group type \***

Security

**Group description** ⓘ  
Enter a description for the group

**Membership type** ⓘ  
Assigned

**Owners**  
No owners selected

**Members**

Ustalamy uprawnienia dla AAzure dlatego wybieramy Security.

Utworzyliśmy grupę CoAdmins:

Search resources, services, and docs (G+/)

Home > Default Directory > Groups | All groups

### Groups | All groups

Default Directory - Azure Active Directory

+ New group Download groups Delete Refresh Preview info Columns Got feedback?

Successfully created group  
Successfully created group CoAdmins.

Name	Object Id	Group Type	Membership Type	Email	Source
CoAdmins	e2d46b9b-3b02-4cad-a...	Security	Assigned		Cloud

Przypiszemy usera do grupy:

https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/UsersManagement

Search resources, services, and docs (G+/)

Home > Default Directory > Users

### Default D... Documentation

Overview Getting started Diagnose and solve problems

Manage

Users

Groups Organizational relationships Roles and administrators

The screenshot shows the Azure Active Directory User Profile page for a user named Peter Blue. The URL is [https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/UserDetailsMenuBlade/Groups/userId/601bcc78-c551-4a59-9e78-85e6c5797266/adminUnitObjectId/](https://portal.azure.com/#blade/Microsoft_AAD_IAM/UserDetailsMenuBlade/Groups/userId/601bcc78-c551-4a59-9e78-85e6c5797266/adminUnitObjectId/).  
The left sidebar has a red box around the 'Groups' link under the 'Manage' section. The main content area shows Peter Blue's profile picture (PB), sign-in history from April 5 to April 26, and his identity details: Name (Peter Blue), First name (Peter), Last name (Blue), User name (peter@examaz900gmail.onmicrosoft.com), User type (Member), Object ID (601bcc78-c551-4a59-9e78-85e6c5797266), and Source (Azure Active Directory).  
The 'Job info' section shows Job title (---), Department (---), and Manager (---).

The screenshot shows the Azure Active Directory User Groups page for Peter Blue. The URL is [https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/UserDetailsMenuBlade/Groups/userId/601bcc78-c551-4a59-9e78-85e6c5797266/adminUnitObjectId/](https://portal.azure.com/#blade/Microsoft_AAD_IAM/UserDetailsMenuBlade/Groups/userId/601bcc78-c551-4a59-9e78-85e6c5797266/adminUnitObjectId/).  
The left sidebar has a red box around the 'Groups' link under the 'Manage' section. The top navigation bar includes links for Azure Active Directory, Azure Multi-Factor Auth, What is Conditional Access, Application Management, and Azure Active Directory. The main content area shows a button '+ Add memberships' with a red box around it. Below it is a message: 'Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview.' A table lists group membership details: Name, Object Id, Group Type, and Membership Type. The table shows 'Not a member of any groups'.

Teraz przypiszemy uprawnienia do grup:

Search resources, services, and docs (G+)

Home > Default Directory | Overview

**Default Directory | Overview**

Azure Active Directory

Overview

Getting started

Diagnose and solve problems

Manage

- Users
- Groups
- Roles and administrators (Preview)** (highlighted with a red box)
- Administrative units (Preview)
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses

Azure AD Connect

Tenant ID: 6e0e4860-6617-4def-a043-f80209197327

Status: Not enabled

Last sync: Sync has never run

Your role: Global administrator More info

Azure AD Free

Definiujemy członkostwo w rolach. Role czyli czynności jakie można wykonywać na portalu. Interesuje nas rola Global administrators. Dla tej roli jednak nie można dodać grupy, można dodawać userów:

Search resources, services, and docs (G+)

Home > Default Directory | Roles and administrators (Preview) > Global administrator | Assignments

**Global administrator | Assignments**

All roles

Diagnose and solve problems

Manage

Assignments

Description

Troubleshooting + Support

New support request

**Add assignments**

+ Add assignments

Remove assignments

Refresh

Search by name

Type: All

Name	UserName
Exam AZ-900	exam.az.900@gmail.com

PB Peter Blue peter@examaz900@gmail.onmicrosoft.com

Selected items

No items selected

Nadamy teraz role resource grupie:

**Add role assignment**

**Role**  Owner

Owner  Lets you view everything, but not make any changes.

Contributor  Lets you change settings and add or remove other users.

Reader  Lets you view everything.

AcrDelete

AcrImageSigner

AcrPull

AcrPush

AcrQuarantineReader

AcrQuarantineWriter

API Management Service Contributor

API Management Service Operator Role

API Management Service Reader Role

App Configuration Data Owner

App Configuration Data Reader

Application Insights Component Contributor

Application Insights Snapshot Debugger

Attestation Contributor

**Role assignments**

Manage access to Azure resources for users, groups, service principals and managed identities at this subscription.

Number of role assignments for this subscription: 0 / 2000

Name	Type	Role
Owner		Owner
Exam AZ-900 exam.az-900_gmail.com#EXT#@examaz900gma...	User	Owner

Owner ma wszystkie uprawnienia, Contributor też ale nie może nadawać uprawnień, Reader – uprawnienie do wylutowania i odczytania wszystkiego.

Wybieramy komu chcemy nadać uprawnienia:

**Add role assignment**

**Role**  Contributor

**Assign access to**  Azure AD user, group, or service principal

**Select**  Search by name or email address

- CityDevAdmins
- CoAdmins
- Exam AZ-900  
exam.az-900\_gmail.com#EXT#@examaz900gma...
- Peter Blue  
peter@examaz900gma.onmicrosoft.com

Selected members:  
No members selected. Search for and add one or more members you want to assign to the role for this resource.

Zalogowaliśmy się nowo stworzonym userem ale widzimy, że nie widzi on wszystkich Resource groups:

The screenshot shows the Microsoft Azure Resource groups page. On the left, there's a sidebar with options like 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. Under 'FAVORITES', 'Resource groups' is selected. The main area is titled 'Resource groups' and shows one record: 'CityDev'. It has a 'Subscription' of 'Free Trial' and is located in 'East US'. There are buttons for 'Add', 'Manage view', 'Refresh', 'Export to CSV', 'Assign tags', and 'Feedback'.

Żeby je widział nie wystarczy, że jest administratorem. Musi mieć też dostęp do subskrypcji. Poprawimy to. Przechodzimy do subskrykcji, Access control, Role assignment i dodajemy grupę naszego usera w roli reader:

The screenshot shows the 'Access control (IAM)' page for the 'Free Trial' subscription. In the left sidebar, 'Access control (IAM)' is highlighted. The main area shows the 'Role assignments' tab. A new role assignment is being created, with 'Reader' selected as the role and 'Azure AD user, group, or service prin...' selected as the assignee. The 'Selected members:' section shows the 'CoAdmins' group selected. At the bottom, there are 'Save' and 'Discard' buttons.

Ten sposób podejścia do definiowania bezpieczeństwa to role base access control.

Azure Active Directory to centralne miejsce z którego sterujemy bezpieczeństwem naszego rozwiązania. To tutaj nadajemy/ odbieramy uprawnienia użytkownikom. Azure AD może się synchronizować z AD on premises.

## Azure AD – bardziej zaawansowane możliwości

Azure AD jest elastyczne, rozbudowane, dostosowane dla nie wielkich i wielkich korporacji, ma współpracować z innymi dostawcami usług i uwierzytelnienia. Funkcjonalność Azure AD może podlegać audytowi. Mamy różne plany według których możemy korzystać z Azure AD:

Currency:  
US Dollar (\$)

	FREE	OFFICE 365 APPS	PREMIUM P1	PREMIUM P2
<b>Core Identity and Access Management</b>				
Directory Objects <sup>1</sup>	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit
Single Sign-On (SSO) <sup>2</sup>	up to 10 apps	up to 10 apps	unlimited	unlimited
User provisioning	✓	✓	✓	✓
Federated Authentication (ADFS or 3rd party IDP)	✓	✓	✓	✓
User and group management (add/update/delete)	✓	✓	✓	✓
Device registration	✓	✓	✓	✓
Cloud Authentication (Pass-Through Auth, Password Hash sync, Seamless SSO)	✓	✓	✓	✓

Ograniczenie opcji free to ilość obiektów jakie można utworzyć.

W opcji free SSO ma ograniczoną ilość aplikacji z jakimi może być sparowane.

Ponadto usługi zależą od wersji subskrypcji i mogą być nie dostępne dla wersji free.

W wersji free nie można synchronizować pomiędzy Azure AD a AD on premises.

Dostępne usługi:

Azure Multi-Factor Authentication – user uwierzytelnia się loginem, hasłem oraz jakimś urządzeniem np. telefon, albo keypass. Może też bazować na biometryce.

The following additional forms of verification can be used with Azure Multi-Factor Authentication:

- Microsoft Authenticator app
- OATH Hardware token
- SMS
- Voice call



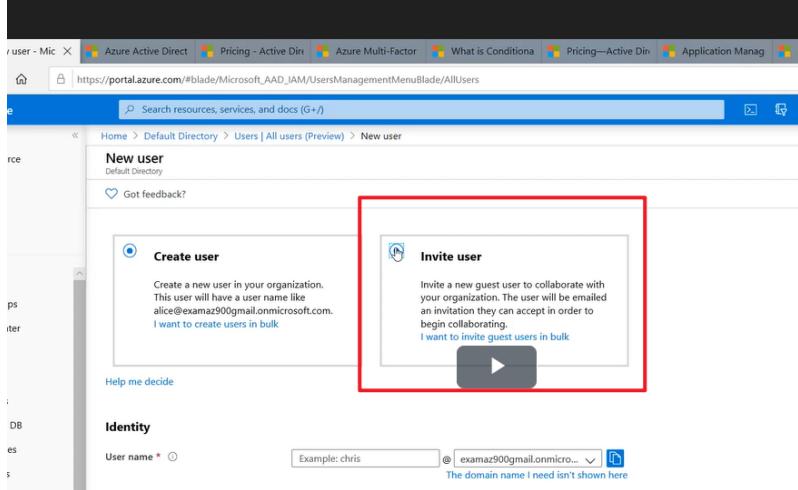
Multi Factor Authentication powinno być włączone dla Global adminów bo oni mają duże uprawnienia, może być dla wszystkich a może być dla wszystkich próbujących dostać się do określonego zasobu – w tym przypadku służy do tego conditional access.

Conditional access – użytkownik loguje się z zewnątrz lub z wewnętrz, korzysta z komputera lub aplikacji itd. Wszystkie czynniki warunkują jak będzie się autentykował. W ten sposób możemy określić jak należy się logować żeby wykonać określone zadania. Możemy blokować użytkowników którzy nie znajdują się w określonej lokalizacji itd.

Azure Active Directory B2C – business to customer – zasoby zdefiniowane w Azure będą udostępniane klientom. Uciążliwie jest gdy wchodząc na stronę nowego sklepu musimy zakładać konto. Można to załatwić poprzez posiadanie konta na innej platformie np. Facebook czy Google. I to jest właśnie Azure

Active Directory B2C. Nie da się tego po prostu włączyć w ustawieniach AD, potrzebna jest specjalna konfiguracja aplikacji.

Azure Active Directory B2B – dwa podmioty mogą realizować jeden projekt i potrzebna jest kooperacja. Aby to zrobić przechodzimy do miejsca w AD, gdzie tworzy się nowych użytkowników ale wybieramy invite user:



The screenshot shows the 'New user' blade in the Azure Active Directory portal. It displays two main options: 'Create user' and 'Invite user'. The 'Invite user' option is highlighted with a red box. Below each option, there is a brief description and a 'Help me decide' button. The 'Identity' section is visible at the bottom, showing a user name input field.

Ostatnia usługa – synchronizacja Azure AD z AD on premises. Mechanizm działania tych dwóch AD jest inny. Azurowe jest otwarte na uwierzytelnienie zewnętrznych dostawców, AD on premises nie jest. Ta funkcjonalność ma znaczenie dla firm przechodzących z on premises do Azure.

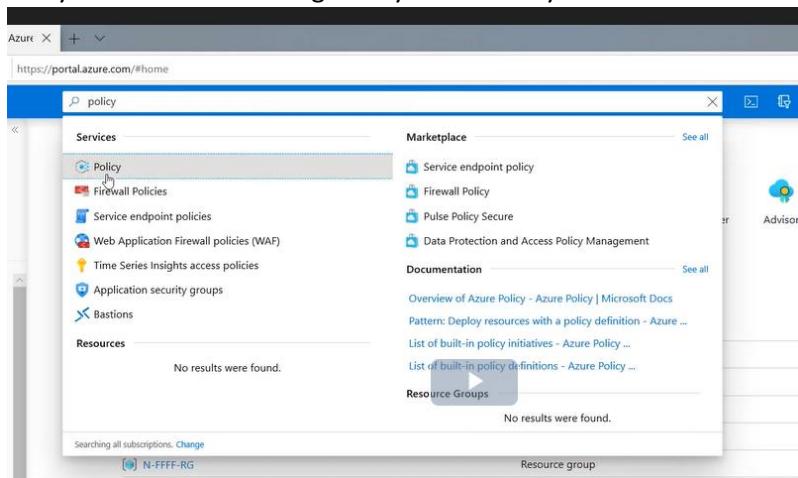
Po skonfigurowaniu takiego połączenia domyślnie synchronizuje się tylko z Azure do on premises.

Ponadto żeby user z Azure został zreplikowany do AD to musi zmienić swoje hasło.

Aby synchronizować w drugą stronę używany jest program Azure AD Connect.

## Policy na straży zachowania reguł

Jedną subskrypcją może administrować wiele osób. Problem jest w tym żeby robili to jednakowo. Odpowiedni opis zasobów, wybór tych samych rodzajów maszyn wirtualnych, tworzenie zasobów takich samych rozmiarów. Do tego służy Azure Policy.



The screenshot shows the Azure portal search results for 'policy'. The 'Services' section is expanded, showing 'Policy' selected. Other items listed include 'Firewall Policies', 'Service endpoint policies', 'Web Application Firewall policies (WAF)', 'Time Series Insights access policies', 'Application security groups', and 'Bastions'. The 'Marketplace' and 'Documentation' sections are also visible.

Mamy zaimplementowane polityki i wskaźnik mówiący o zgodności z tymi politykami:

The screenshot shows the Azure Policy Overview page. The main dashboard displays the following metrics:

- Overall resource compliance: 91% (179 out of 197)
- Non-compliant initiatives: 1 (out of 1)
- Non-compliant policies: 38 (out of 99)
- Non-compliant resources: 18 (out of 197)

A table below lists the assigned policy details:

Name	Scope	Compliance state	Resource compli...	Non-Compliant Res...	Non-compliant polic...
ASC Default (subscription: 08c2a365-709...	Free Trial	Non-compliant	91% (179 out of 197)	18	38

Below the table is a chart titled "ASSIGNMENTS BY COMPLIANCE (LAST 7 DAYS)" showing the number of assignments over time.

Stworzymy sobie własne policy:

The screenshot shows the Azure Policy Assignments page. The main dashboard displays the following metrics:

- Total Assignments: 1
- Initiative Assignments: 1 (1)
- Policy Assignments: 0

A table below lists the assigned policy details:

Name	Scope	Type
ASC Default (subscription: 08c2a365-709...	Free Trial	Initiative

The left sidebar shows the navigation menu, and the "Assignments" section is highlighted with a red box. The "Assign policy" button is also highlighted with a red box.

Policy jest przypisane do subskrypcji ale można wskazać zasoby, które mają nie podlegać policy. Można różnoraką budować definicję polityki ale można też wzorować się na predefiniowanych policy. Np. dostępne lokalizacje dla COsmos DB:

My wybieramy inherit tag from resource group:

Jeżeli do grupy zasobów przypiszemy tag to będzie on dziedziczony przez obiekty jakie w tej grupie się znajdują.

Możemy włączyć policy enforcement – spowoduje to że jeśli spróbujemy zrobić coś wbrew regule to taka operacja się nie uda:

Search resources, services, and docs (G+/)

Home > Policy | Assignments > Assign policy

## Assign policy

Scope Learn more about setting the scope

Free Trial

Exclusions

Optionally select resources to exempt from the policy assignment

**Basics**

Policy definition \*

Inherit a tag from the resource group

Assignment name \* ⓘ

Inherit a tag from the resource group

Description

When enforcement mode is disabled, the policy effect isn't enforced (i.e. deny policy won't deny resources). Compliance assessment results are still available.  
<https://aka.ms/enforcementMode>

Policy enforcement ⓘ

Enabled  Disabled

Assigned by

Exam AZ-900

Tutaj określmy jaki tag ma być dziedziczone:

Assign policy

Basics Parameters Remediation Review + create

Specify parameters for this policy assignment.

Tag Name \* ⓘ

Review + create Cancel Previous Next

Sprawdzamy stan zdefiniowanej policy:

The screenshot shows the Azure Policy Overview page for a scope named "Free Trial". Key statistics displayed are:

- Overall resource compliance: 90% (179 out of 198)
- Non-compliant initiatives: 1 out of 1
- Non-compliant policies: 38 out of 100
- Non-compliant resources: 19 out of 198

A table lists non-compliant resources:

Name	Scope	Compliance state	Resource compli...	Non-Compli...
ASC Default (subscription)	Free Trial	Non-compliant	90% (179 out of 198)	19
Inherit a tag from the res...	Free Trial	Not started	100% (0 out of 0)	0

The row for "Inherit a tag from the res..." is highlighted with a red box.

## Locks

Locks – chronią przed niechcianym usunięciem.

Definiujemy Lock na Resource Grupie:

The screenshot shows the Azure Resource Group settings page for "CityDev". The "Locks" section is highlighted with a red box. A modal window titled "Add lock" is open, showing the configuration for a new lock:

- Lock name: DontChange
- Lock type: Read-only
- Notes: Don't change without contacting the owner

The "OK" button is visible at the bottom of the modal.

Próbujemy usunąć tag maszyny wirtualnej i nie da rady:

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case-insensitive and tag values are case-sensitive. [Learn more about tags](#)

Name	Value	Actions
Application	: SoftwareDev	...
Department	: Developers	...
Environment	: DEV	...
Owner	: Ann Keller	...

Locki można zakładać nie tylko na grupę zasobów ale na same zasoby, które znajdują się w grupie.

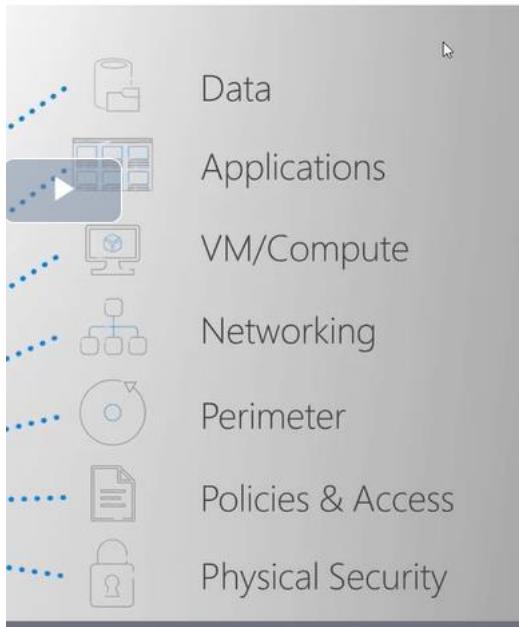
## Migracja do chmury a kwestie bezpieczeństwa

Microsoft zbudował Cloud Adoption Framework aby ułatwić wyjaśnienie, że chmura to rozwiązanie bezpieczne, skalowalne i niedrogie.

Cloud Adoption Framework – to proponowane ramy migracji do Azure w postaci kolejnych kroków jakie należy przejść. Na tej stronie znajdują się informacje co może motywować niezdecydowane firmy do migracji do chmury. Są też informacje o narzędziach jakie mają ułatwić proces migracji.

Organizacja bezpieczeństwa chmury została podzielona na kilka warstw:

- fizyczne bezpieczeństwo
- polityki i ograniczenia dostępu
- ochrona sieci
- zabezpieczenia na poziomie sieci
- zabezpieczenia maszyn
- zabezpieczenia aplikacji
- zabezpieczenia danych



Są 3 główne cechy zabezpieczenia danych:

- confidentiality – dostęp mają mieć ci którzy naprawdę ich potrzebują – najniższy przywilej

Uwierzytelnienie – authentication – sprawdzenie kim jesteś

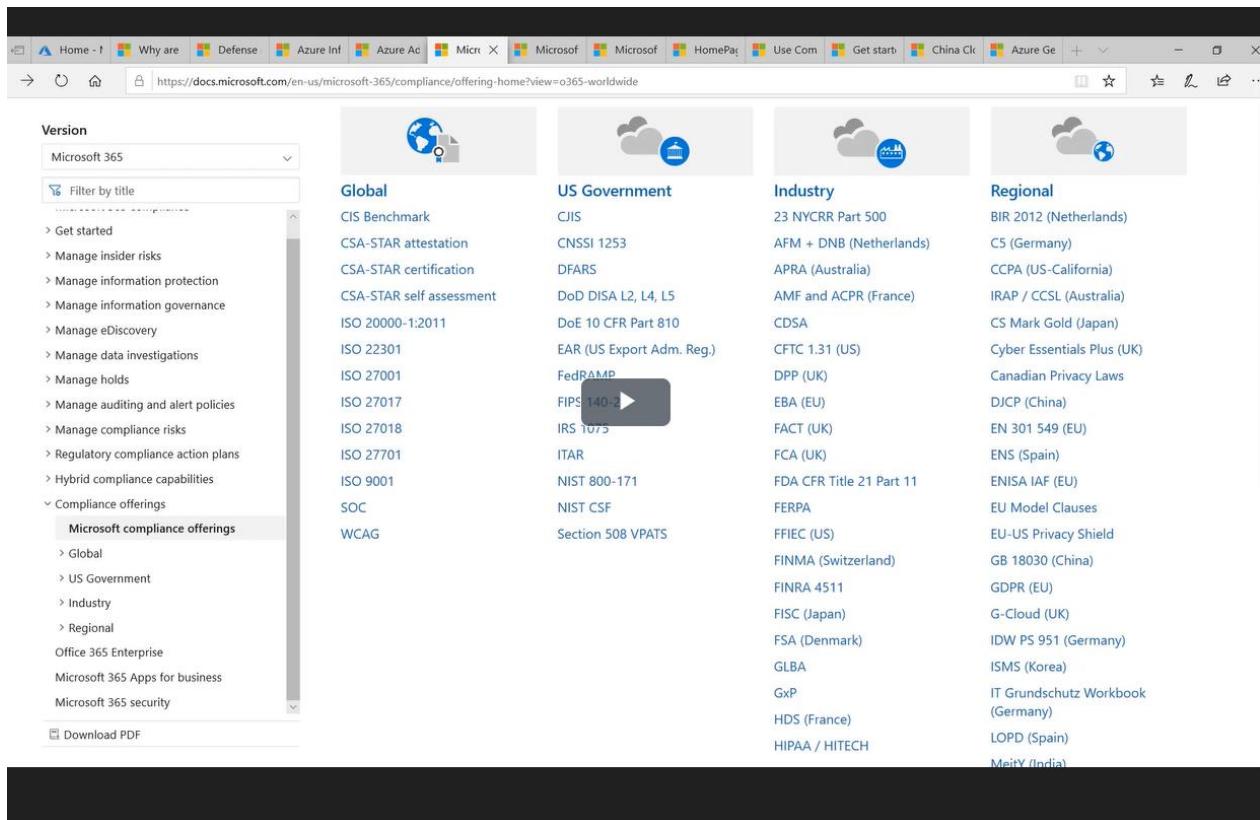
Autoryzacja – authorization – sprawdzenie czy masz dostęp do danego zasobu, czy możesz zrobić to co chcesz zrobić. Autoryzacja wymaga wcześniejszego uwierzytelnienia.

- integrity – zapobieganie nieporządanym zmianom
- availability – dane powinny być dostępne

Azure information Protection – usługa do zabezpieczania danych elektronicznych – np. pilnowanie czy mail nie został wysłany do niewłaściwej osoby albo blokada możliwości wydruku załącznika

Azure Advanced Thread Protection – analiza zachowania użytkowników a następnie klasyfikacja na takie które są podejrzane i takie które są zwykłą działalnością użytkownika

Microsoft postarał się o pozytywne wyniki audytu i compliance:



The screenshot shows a list of compliance offerings for Microsoft 365. The offerings are organized into four main categories: Global, US Government, Industry, and Regional. Each category contains several specific compliance standards or frameworks. A search bar and a download PDF button are also visible.

Category	Offering
Global	CIS Benchmark
	CSA-STAR attestation
	CSA-STAR certification
	CSA-STAR self assessment
	ISO 20000-1:2011
	ISO 22301
	ISO 27001
	ISO 27017
	ISO 27018
	ISO 27701
US Government	DoD DISA L2, L4, L5
	ISOE 10 CFR Part 810
	EAR (US Export Adm. Reg.)
	FedRAMP
	FIPS 140-2
	IRS 1075
	ITAR
	NIST 800-171
	NIST CSF
	Section 508 VPATs
Industry	23 NYCRR Part 500
	AFM + DNB (Netherlands)
	APRA (Australia)
	AMF and ACPR (France)
	CDSA
	DPP (UK)
	EBA (EU)
	FACT (UK)
	FCA (UK)
	FDA CFR Title 21 Part 11
Regional	CS Mark Gold (Japan)
	Cyber Essentials Plus (UK)
	Canadian Privacy Laws
	DJCP (China)
	EN 301 549 (EU)
	ENS (Spain)
	ENISA IAF (EU)
	EU Model Clauses
	EU-US Privacy Shield
	GB 18030 (China)

CJIS – Criminal Justice Information Services dostęp do danych FBI

CSA-STAR – zgodność z ISO, spełnienie wymogów dotyczących krytycznych zdarzeń dotyczących bezpieczeństwa

GDBR – RODO dane osobowe

EU Model Clauses – zasady przetwarzania danych z unii europejskiej

HIPAA – dostęp do danych dotyczących zdrowia i ubezpieczeń społecznych

ISO 27018 – zasady przetwarzania informacji personalnych

SOC – service organization controls – audyt coroczny, bezpieczeństwo, dostępność, integralność, poufność danych

NIST CSF – national institute of standard and technology cyber security framework

G-CLOUD – przedstawianie danych I przedsiębiorstw obywateli UK

MTCS – w Singapurze, certyfikowana platforma dfo świadczenia usług

Największym klientem Microsoftu są rządy. Często chcą one mieć wydzieloną chmurę w której ich dane będą przetwarzane na obszarze ich kraju tylko przez obywateli swojego kraju, tylko i wyłącznie zasobami tego kraju. W chinach Azure musi współpracować ze spółką 21Vianet. W chinach to właśnie za pośrednictwem tej firmy można kupić usługi. Rządy kupują usługi Azure kontaktując się bezpośrednio z serwisem. Poza tym są 3 drogi zakupu:

- przez stronę internetową
- przez partnera Microsoft
- specjalne umowy dla wielkich firm – enterprise agreement

## **Service Level Agreement, Technical Support**

Każda z usług jest objęta umową między mną a dostawcą. Ta umowa nazywa się service level agreement (SLA). Właściwie to dla każdego zasobu istnieje osobna umowa, która określa co i jak działa. Każda umowa jest opisana na stronie Microsoftu. Sprawdzamy jak wygląda dostępność maszyny wirtualnej:

- maszyna zinstancjami w więcej niż jednej Availability Zone – 99.99%
- maszyna zinstancjami w tym samym Availability Set – 99.95%
- pojedyncza instancja 99.9%

Wyliczany jest miesięczny uptime:

**Monthly Uptime % = (Maximum Available Minutes – Downtime) / Maximum Available Minutes X 100**

Jeśli wartość ta spadnie poniżej pewnych poziomów to są wypłacane odszodowania.

Maximum Available Minutes – maksymalny czas w miesiącu.

W przypadku maszyn rozmieszczonych w Availability Zones Microsoft zwraca następującą liczbę środków:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.99%	10%
< 99%	25%
< 95%	100%

W przypadku maszyn rozmieszczonych w Availability Sets Microsoft zwraca następującą liczbę środków:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.95%	10%
< 99%	25%
< 95%	100%

Maszyna pojedyncza:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.9%	10%
< 99%	25%
< 95%	100%

Oprócz SLA poszczególnych usług jest jeszcze SLA kompozytowe – jeśli moje rozwiązania składa się z 2-ch komponentów i pierwsza z maszyn jest dostępna przez 99.9% a druga 99.95% to SLA kompozytowe wynosi  $0.999 \times 0.9995 = 0.9985005$ .

Compare suport plan – wsparcie techniczne. Mamy różne rodzaje planów:



Każdy z planów oferuje dostęp do rachunków, dokumentacji, wysyłania prośb o wsparcie, dostęp do Azure Acessore, sprawdzanie Azura samego w sobie.

Developer – reakcja na usterkę do 8 godzin

Standard, Professional – klasyfikujemy usterki na kategorie A, B i C i jest rekacja po 8/4 , 4/2, 1 godzinach

W planie professional mamy w pakiecie wskazówki od konsultantów czy też szkolenia.

Microsoft tworząc nowe rozwiązania daje je do oceny wybranym klientom. Niedokończone rozwiązania są często dostępne i opisywane są w nazwie przez „Preview”:

The screenshot shows the Microsoft Azure Marketplace search results page. The search bar at the top contains the text 'preview'. Below the search bar, there are filters for 'Pricing : All' and 'Operating System :'. On the left, there is a sidebar with 'My Saved List', 'Recently created', 'Service Providers', and a 'Categories' section where 'Get Started' is highlighted. The main area displays search results under the heading 'Showing All Results'. Three items are listed: 'Office 365 Analytics (Preview)' by Microsoft, 'CrateDB [Preview]' by Crate.IO, and 'Azure SQL Analytics (Preview)' by Microsoft. Each item has a thumbnail, name, provider, and a brief description.

Home > New > Marketplace

Marketplace

My Saved List

Recently created

Service Providers

Categories

Get Started

AI + Machine Learning

Analytics

preview

Pricing : All

Operating System :

Showing All Results

Office 365 Analytics (Preview)

CrateDB [Preview]

Azure SQL Analytics (Preview)