Microsoft 365 CONFERENCE

Microsoft Viva
Microsoft Teams
Microsoft SharePoint
Microsoft Power Platform

CO PRODUCED BY MICROSOFT AND M365 CONFERENCE

MICROSOFT 365 CONFERENCE
Secure your Enterprise applications with Azure

Toni Pohl
Azure and Office Development MVP, CTO atwork
@atwork | toni.pohl@atwork.at | www.atwork-it.com

Get Whova

Official Event App

The event invitation code is: **M365Spring22**

- **Access links** to join all sessions and keynotes virtually
- Explore the **professional profiles** of event speakers and attendees
- Send **in-app messages** and **exchange contact info**
- **Network and find attendees** with common affiliations, educations, shared networks, and social profiles
- Receive **update notifications** from organizers
- Access the **event agenda**, GPS guidance, maps, and parking directions at your fingertips

Plan For Events

See who else is attending and connect
Plan your schedule

Download Whova and take your event mobile.

Get Whova from the App Store or Google Play.

Available on the App Store   GET IT ON Google Play

Please sign up for the app with your social media account or email.

The event invitation code is:
M365Spring22

You will be asked for an event invitation code after installing Whova.

2022

In-Person – April and December

Microsoft 365 CONFERENCE

Microsoft Viva
Microsoft Teams
Microsoft SharePoint
Microsoft Power Platform

CO PRODUCED BY MICROSOFT AND M365 CONFERENCE

April 5 – 7, 2022
MGM Grand
Las Vegas, NV

December, 2022
Check website for details

Moving workloads and data to the cloud?

Customer: “The (public) cloud is not safe”

Consultant: “Azure is secure by default”

Microsoft: “Azure AD, Azure Security Center, Key Vault, VNets, Bastion, WAF, + many more services…”

“Microsoft Azure provides a secure foundation across physical, infrastructure, and operational security.”

- Azure compliance
  https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/
- Compliance offerings
  https://docs.microsoft.com/en-us/azure/compliance/
- Microsoft Security Blog
  https://aka.ms/security
- Blog… Microsoft Azure leads the industry in ISO certifications
  https://azure.microsoft.com/en-us/blog/microsoft-azure-leads-the-industry-in-iso-certifications/

Identify your use cases!

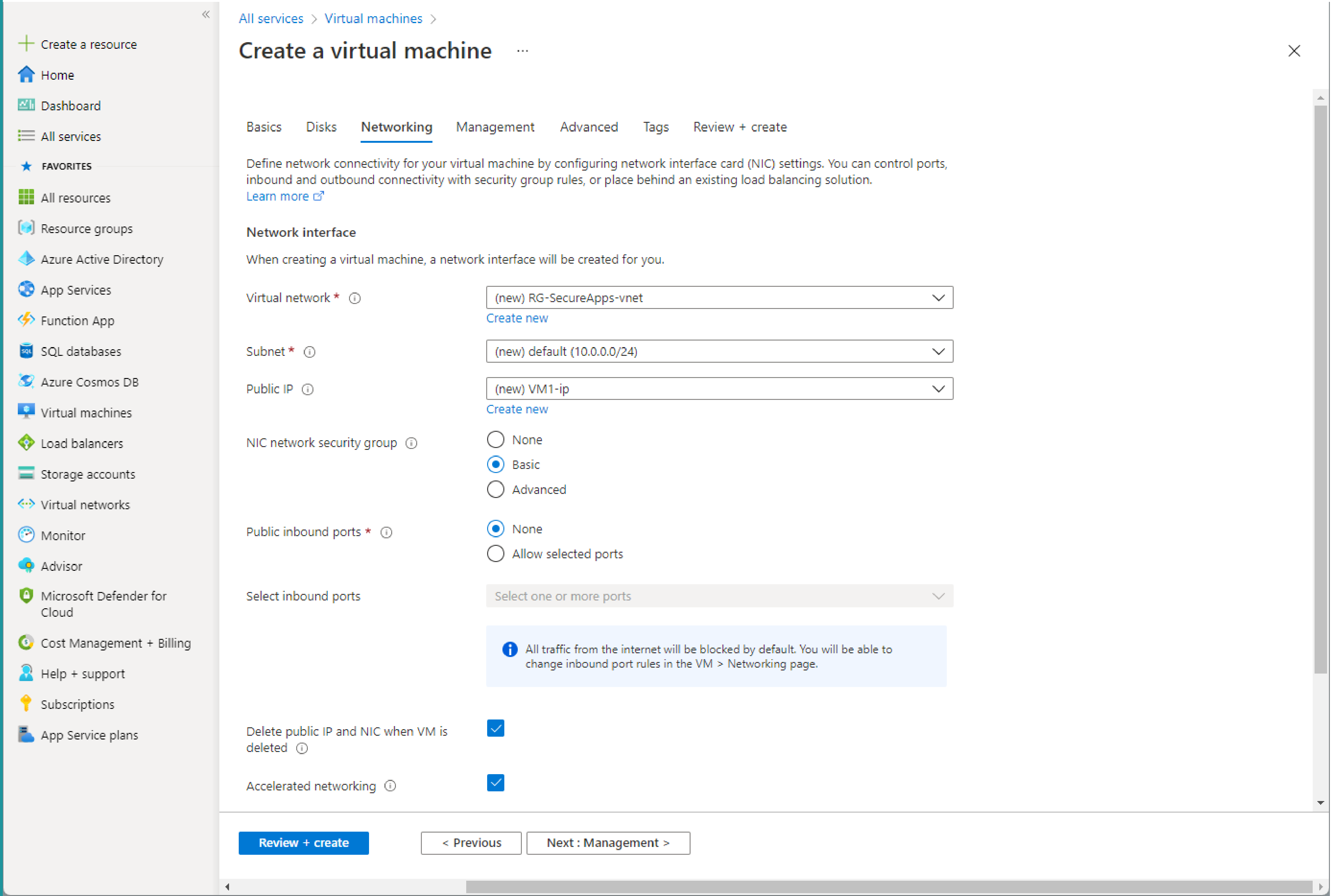
Typical workloads types

- VM´s & Containers
- Web Apps
- PowerShell Scripts
- Business workflows

VM´s

- Check the settings
- Control the access

Create



Create a virtual machine

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 * : (new) RG-SecureApps-vnet
Create new

Subnet * : (new) default (10.0.0.0/24)

Public IP : (new) VM1-ip
Create new

NIC network security group : ○ None ● Basic ○ Advanced

Public inbound ports * : ● None ○ Allow selected ports

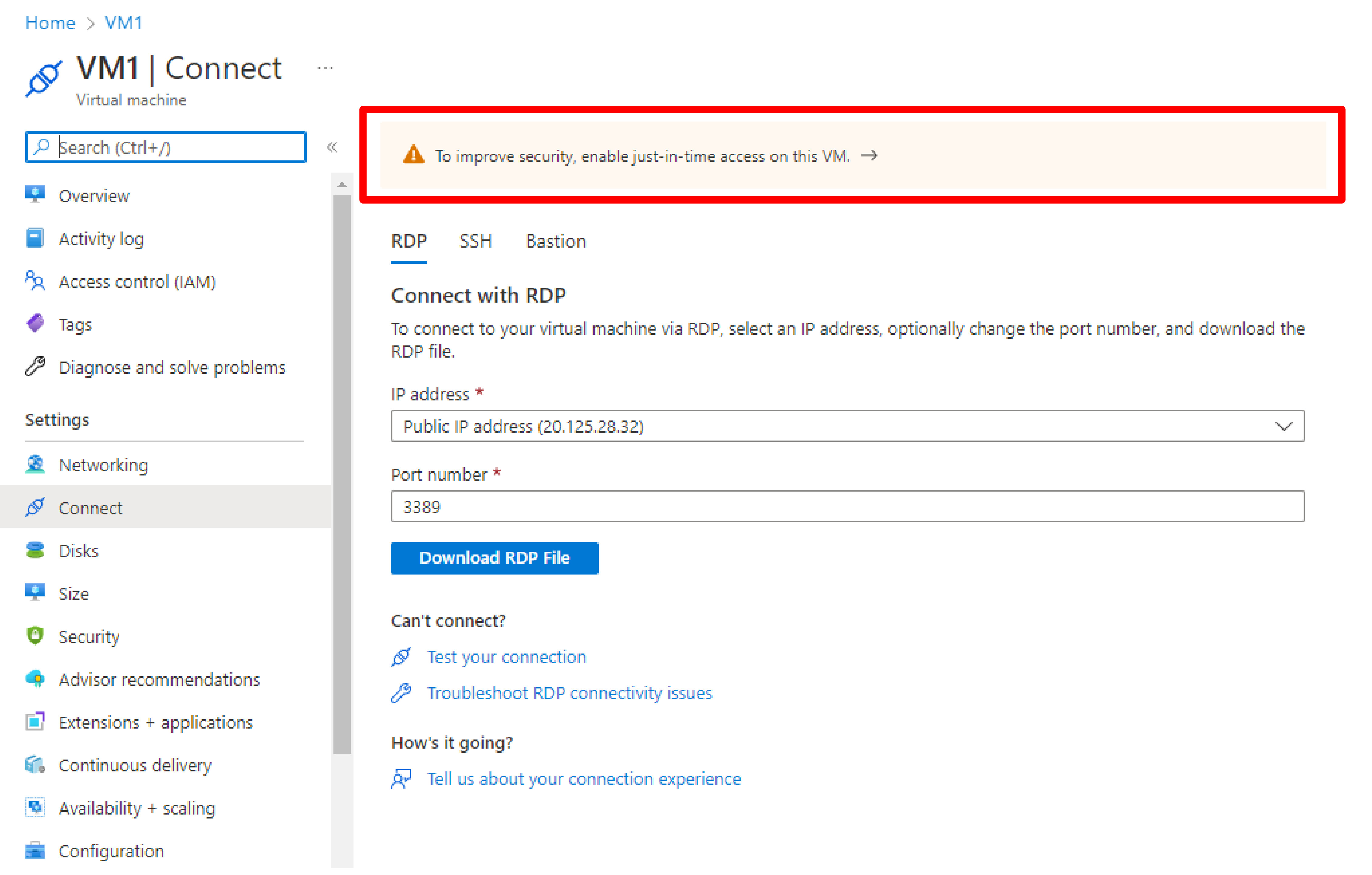
Select inbound ports : Select one or more ports

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

Delete public IP and NIC when VM is deleted ☑

Accelerated networking ☑

JIT



Home > VM1

VM1 | Connect

Virtual machine

⚠ To improve security, enable just-in-time access on this VM. →

Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

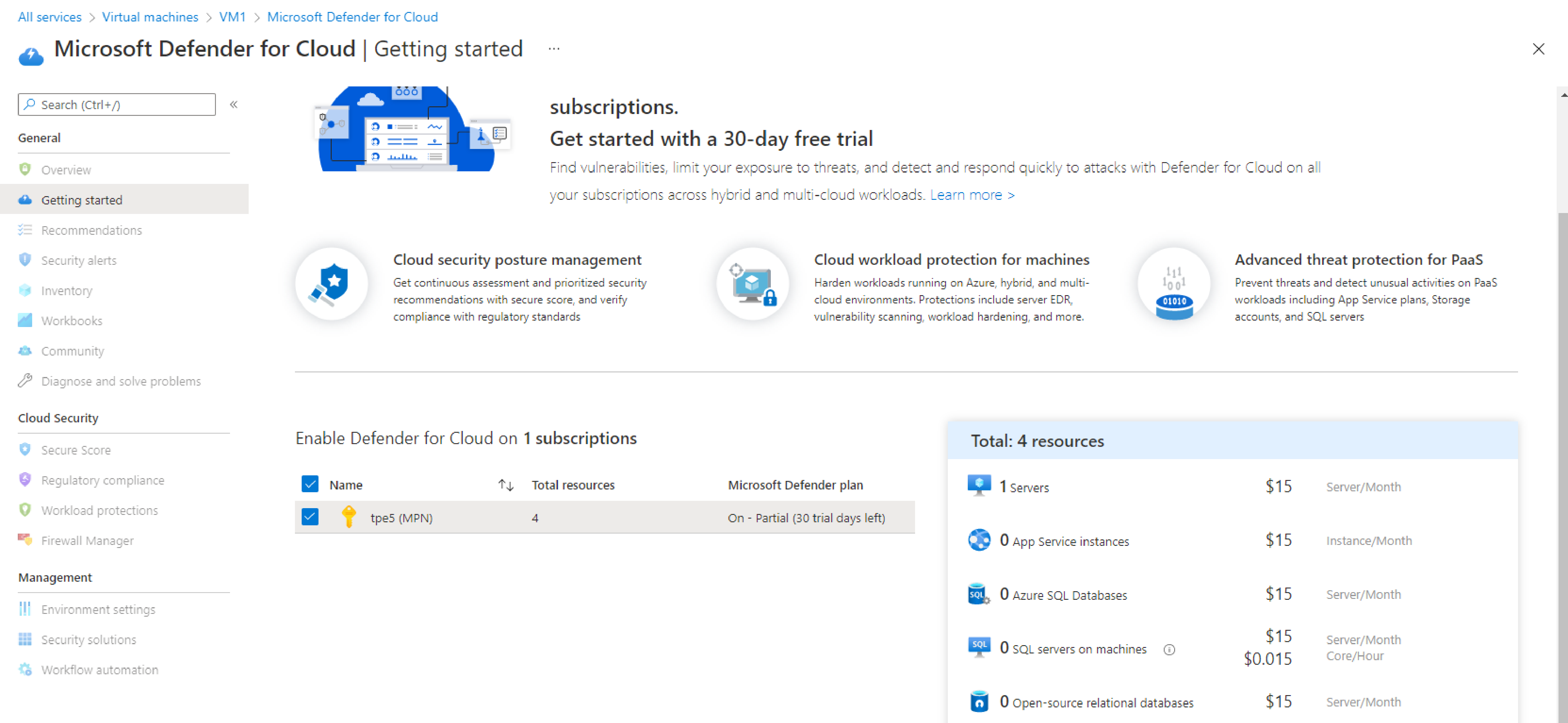
IP address *

Public IP address (20.125.28.32)

Port number *

3389

JIT requires Defender for Cloud



All services > Virtual machines > VM1 > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Getting started ...

subscriptions.

Get started with a 30-day free trial

Find vulnerabilities, limit your exposure to threats, and detect and respond quickly to attacks with Defender for Cloud on all your subscriptions across hybrid and multi-cloud workloads. Learn more >

Cloud security posture management
Get continuous assessment and prioritized security recommendations with secure score, and verify compliance with regulatory standards

Cloud workload protection for machines
Harden workloads running on Azure, hybrid, and multi-cloud environments. Protections include server EDR, vulnerability scanning, workload hardening, and more.

Advanced threat protection for PaaS
Prevent threats and detect unusual activities on PaaS workloads including App Service plans, Storage accounts, and SQL servers

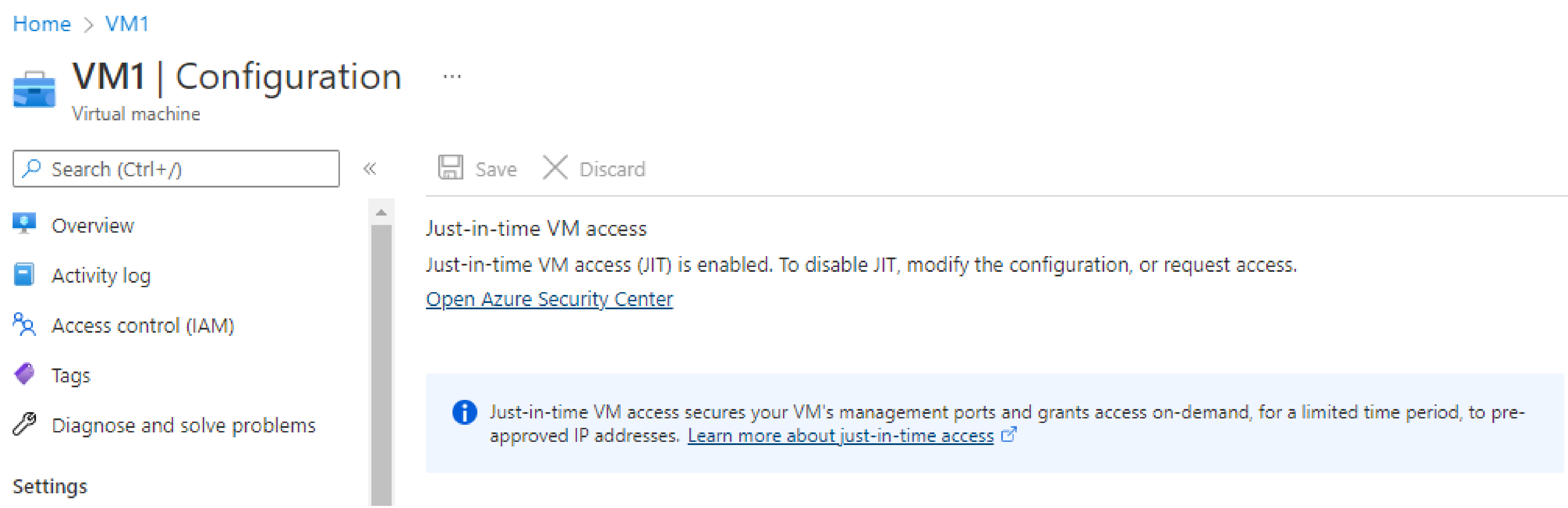
Enable Defender for Cloud on **1 subscriptions**

☑	Name ↑↓	Total resources	Microsoft Defender plan
☑	tpe5 (MPN)	4	On - Partial (30 trial days left)

Total: 4 resources

1 Servers	$15	Server/Month
0 App Service instances	$15	Instance/Month
0 Azure SQL Databases	$15	Server/Month
0 SQL servers on machines ⓘ	$15 $0.015	Server/Month Core/Hour
0 Open-source relational databases	$15	Server/Month

JIT



VM1 | Configuration

Virtual machine

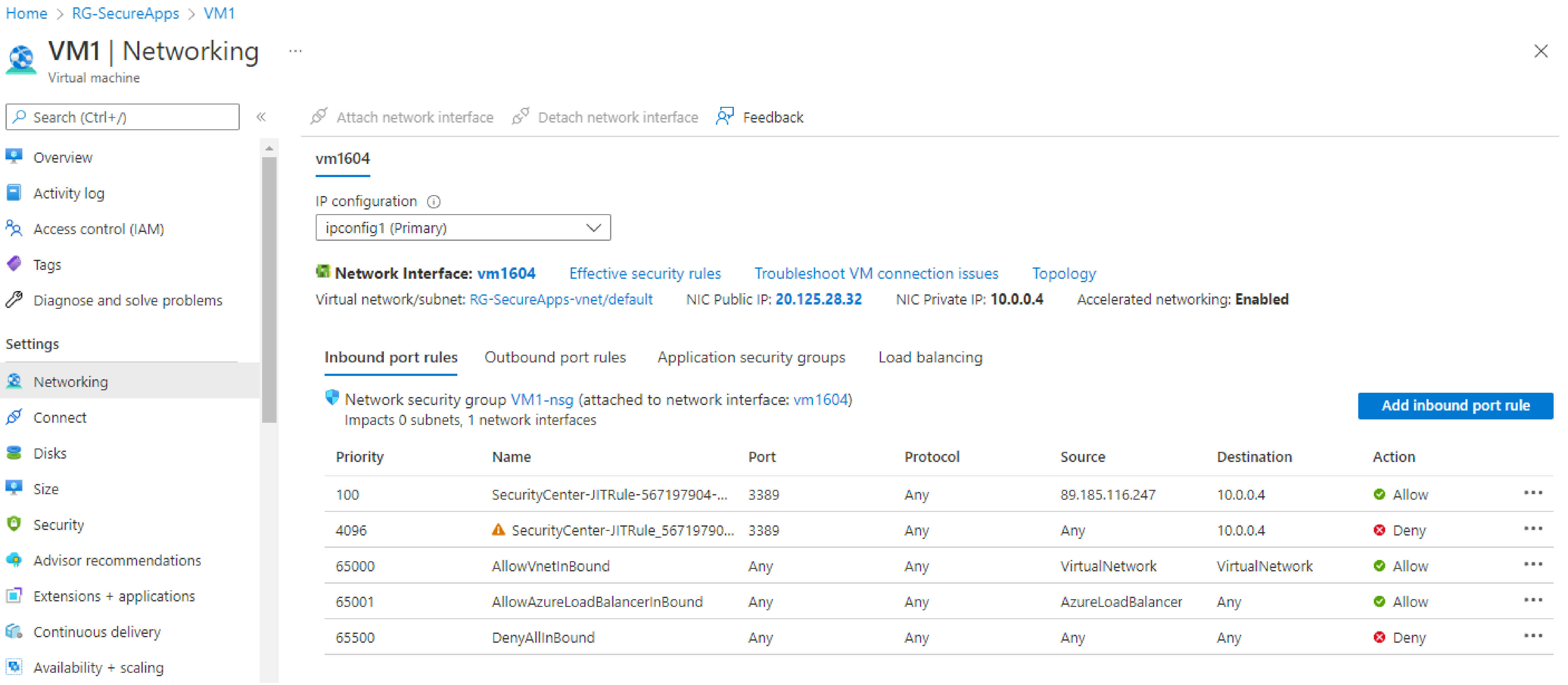
Just-in-time VM access

Just-in-time VM access (JIT) is enabled. To disable JIT, modify the configuration, or request access.

Open Azure Security Center

Just-in-time VM access secures your VM's management ports and grants access on-demand, for a limited time period, to pre-approved IP addresses. Learn more about just-in-time access

JIT creates a temporary rule in the Firewall



VM1 | Networking

Virtual machine

IP configuration: ipconfig1 (Primary)

Network Interface: vm1604

Virtual network/subnet: RG-SecureApps-vnet/default NIC Public IP: 20.125.28.32 NIC Private IP: 10.0.0.4 Accelerated networking: Enabled

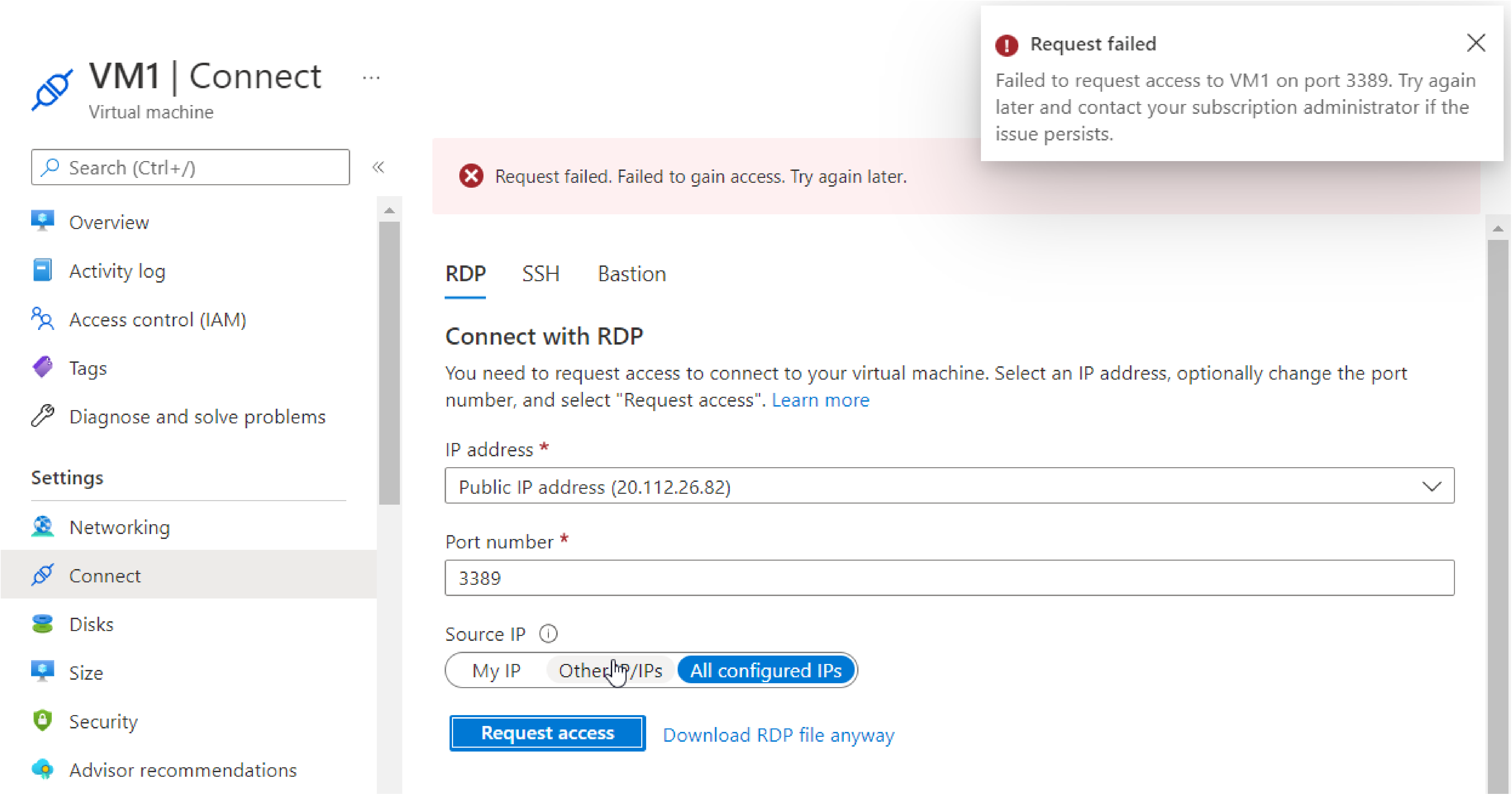
Network security group VM1-nsg (attached to network interface: vm1604)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
100	SecurityCenter-JITRule-567197904-...	3389	Any	89.185.116.247	10.0.0.4	✓ Allow
4096	⚠ SecurityCenter-JITRule_56719790...	3389	Any	Any	10.0.0.4	✗ Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Using Azure policies

- Enforce specific settings

Policy in action



VM1 | Connect

Virtual machine

Request failed

Failed to request access to VM1 on port 3389. Try again later and contact your subscription administrator if the issue persists.

Request failed. Failed to gain access. Try again later.

Connect with RDP

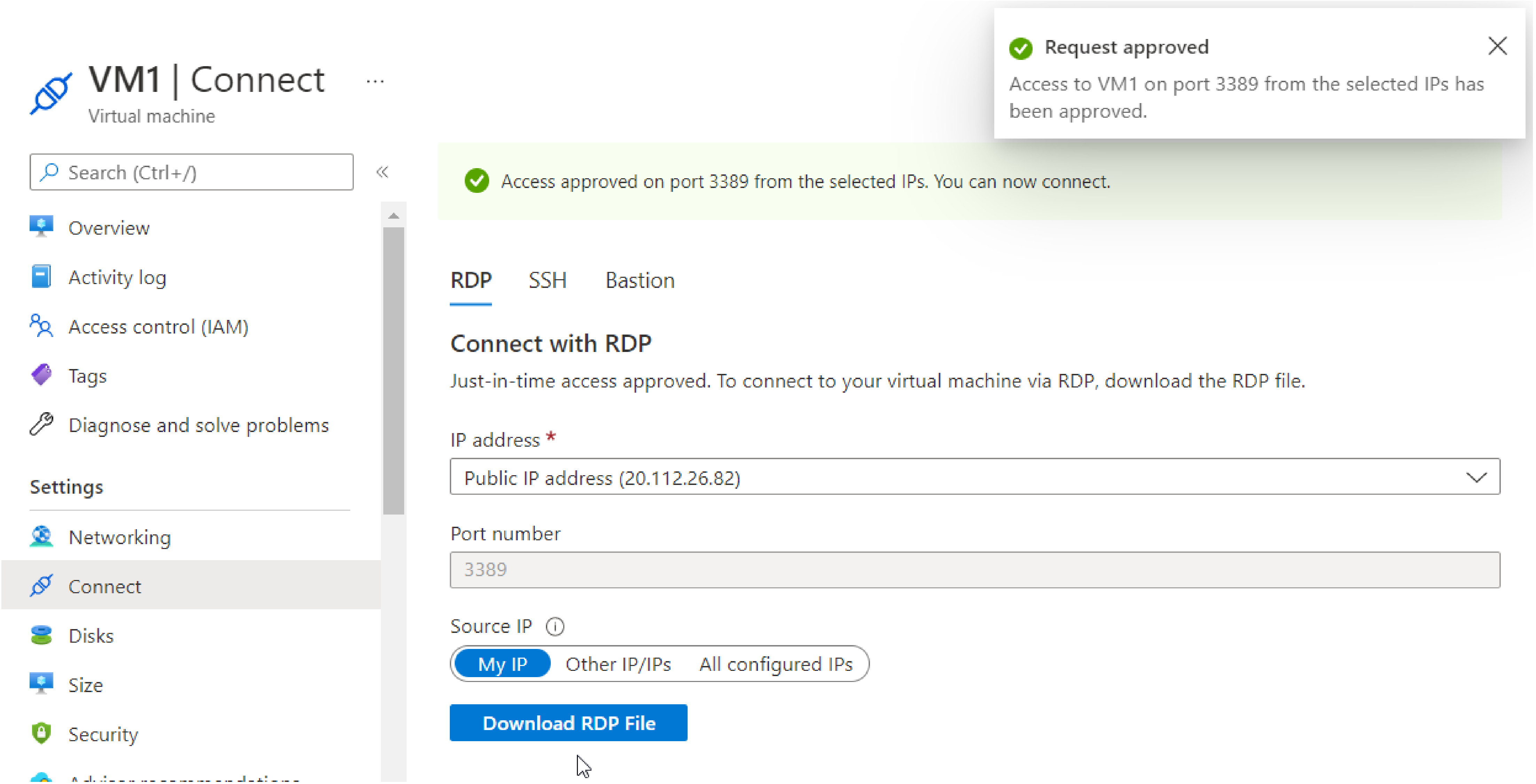
You need to request access to connect to your virtual machine. Select an IP address, optionally change the port number, and select "Request access". Learn more

IP address *: Public IP address (20.112.26.82)

Port number *: 3389

Source IP: ○ My IP ○ Other IP/IPs ● All configured IPs

Policy in action



VM1 | Connect

Virtual machine

Request approved

Access to VM1 on port 3389 from the selected IPs has been approved.

Access approved on port 3389 from the selected IPs. You can now connect.

Connect with RDP

Just-in-time access approved. To connect to your virtual machine via RDP, download the RDP file.

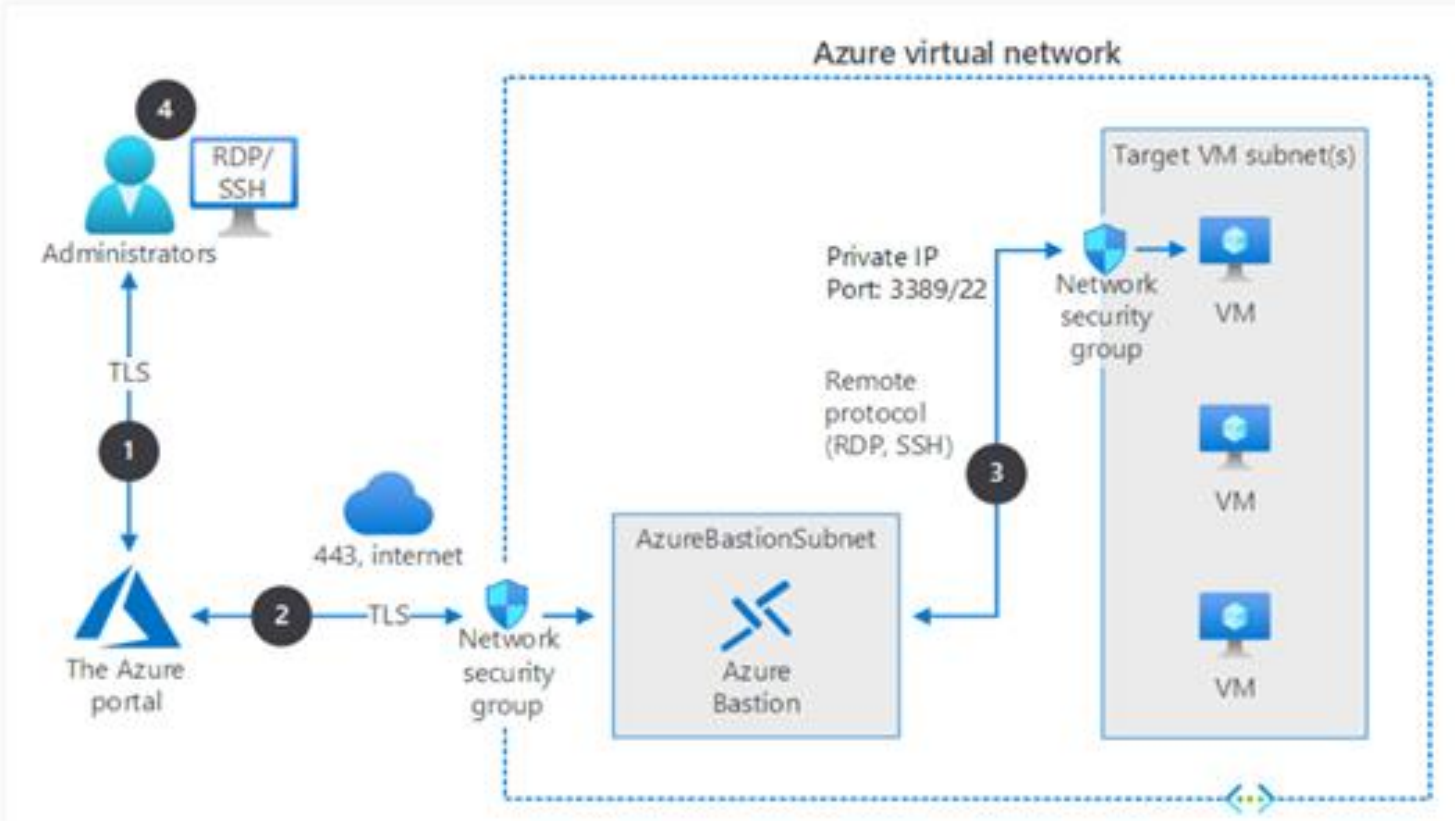
IP address *: Public IP address (20.112.26.82)

Port number: 3389

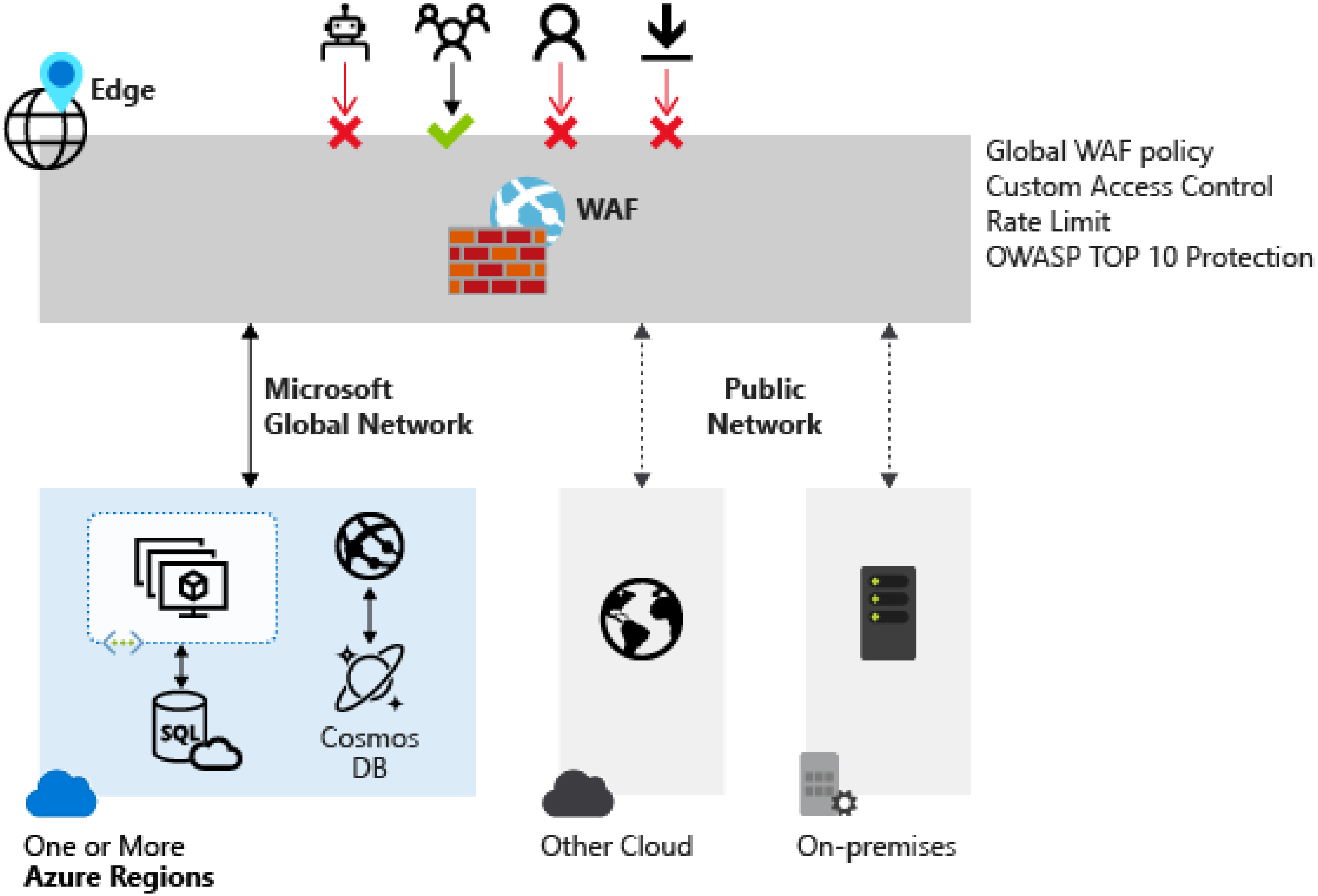
Source IP: [✓ My IP] Other IP/IPs All configured IPs

More services to secure your resources

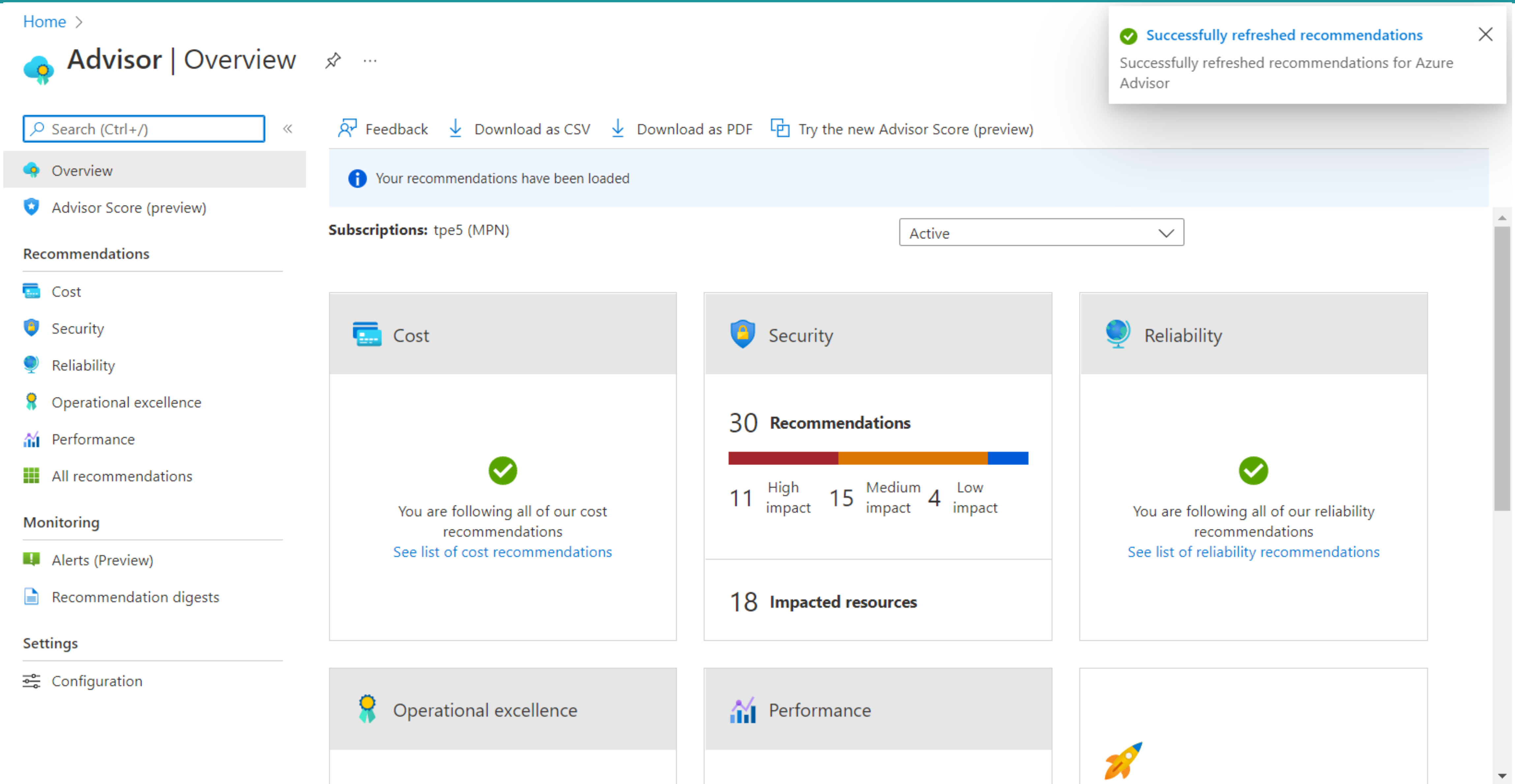
Many VMs: Azure Bastion



Web Application Firewall



Use Azure Advisor



Successfully refreshed recommendations

Successfully refreshed recommendations for Azure Advisor

Your recommendations have been loaded

Subscriptions: tpe5 (MPN)

Active

You are following all of our cost recommendations

See list of cost recommendations

30 **Recommendations**

11 High impact 15 Medium impact 4 Low impact

18 **Impacted resources**

You are following all of our reliability recommendations

See list of reliability recommendations

Identities

In M365/Azure,
the basis is identity…

Users / Apps*

Apps Demo

- Access resources with predefined permissions

Azure Key Vault

- The safe place to store credentials and secrets like connection strings, etc.
- https://docs.microsoft.com/en-us/azure/key-vault/general/security-features

Types of Apps

- App
  Application object is the global representation of your application (for use across all tenants)
- SPN
  The service principal is the local representation for use in a specific tenant. Defines the access policy and permissions for the user/application in the Azure AD tenant. Done when creating an app.
- Managed identity
  Eliminate the need for developers to manage credentials
- [Legacy]: Before Apps management

I can use Managed Identities when…

As a developer, I want to build an application using

Source:

Azure Resources
Azure VMs
Azure App Services
Azure Functions
Azure Container instances
Azure Kubernetes Service
Azure Logic Apps
Azure Storage
….

that accesses

Target:

Any target that supports Azure Active Directory Authentication:

- **Your applications**
- **Azure Services:**
  - Azure Key Vault
  - Azure Storage
  - Azure SQL…

without having to manage any credentials!

For example, I want to build an application using ***Azure App Services*** that accesses **Azure Storage** without having to manage any credentials.

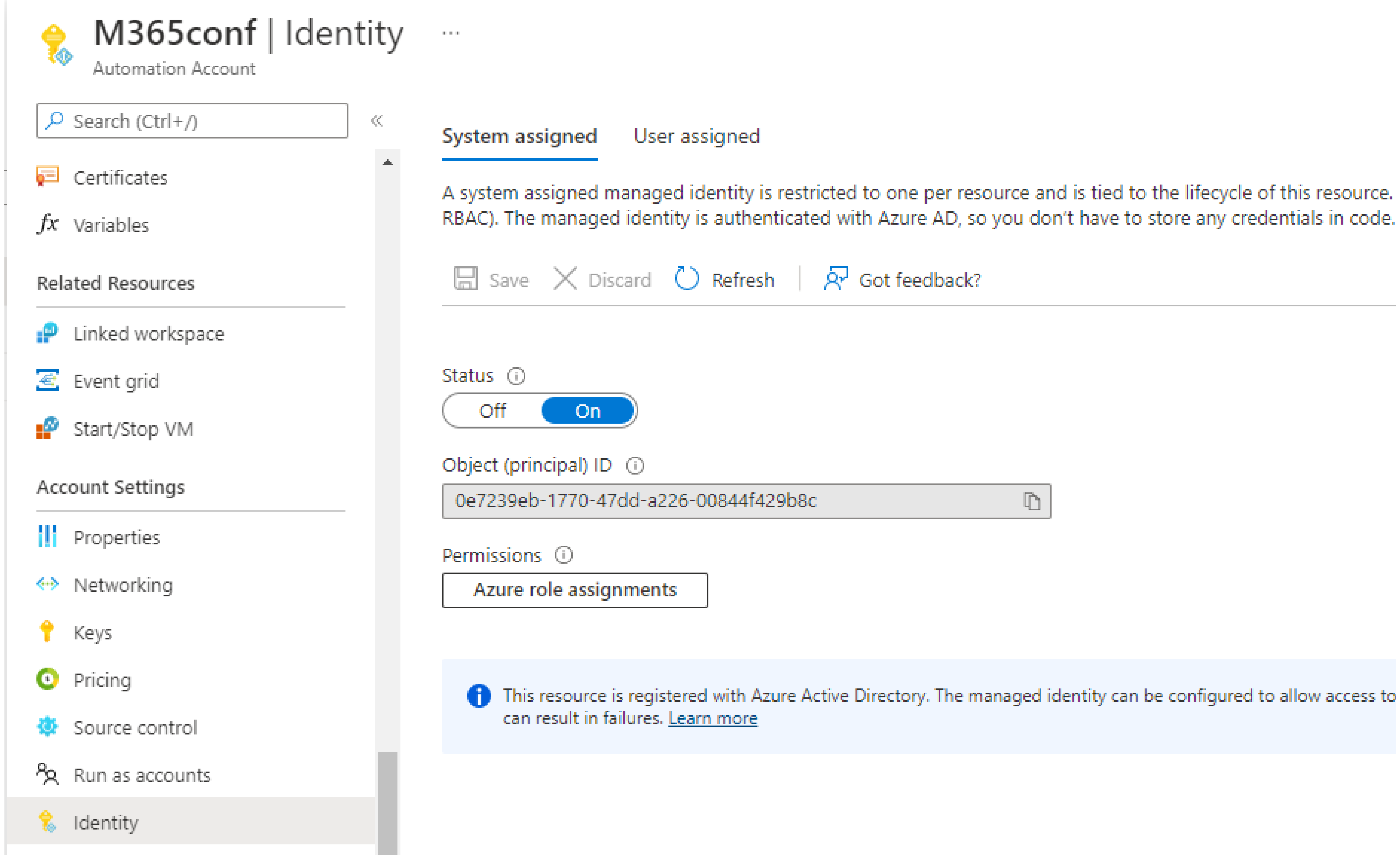
Managed Identity types – when use what?

- System-assigned
    - Tied to the lifecycle of that service instance.
    - Only that Azure resource can use this identity to request tokens from Azure AD.
- User-assigned
    - Managed identity as a standalone Azure resource
    - managed separately from the resources that use it.
    - Assign it to one or more instances of an Azure service

https://docs.microsoft.com/en-us/azure/logic-apps/create-managed-service-identity?tabs=consumption

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/field-notes-remediating-resources-using-user-assigned-managed/ba-p/3258700

Managed Identities



A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource.
RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code.

Status ⓘ

Off [✓ On]

Object (principal) ID ⓘ

0e7239eb-1770-47dd-a226-00844f429b8c

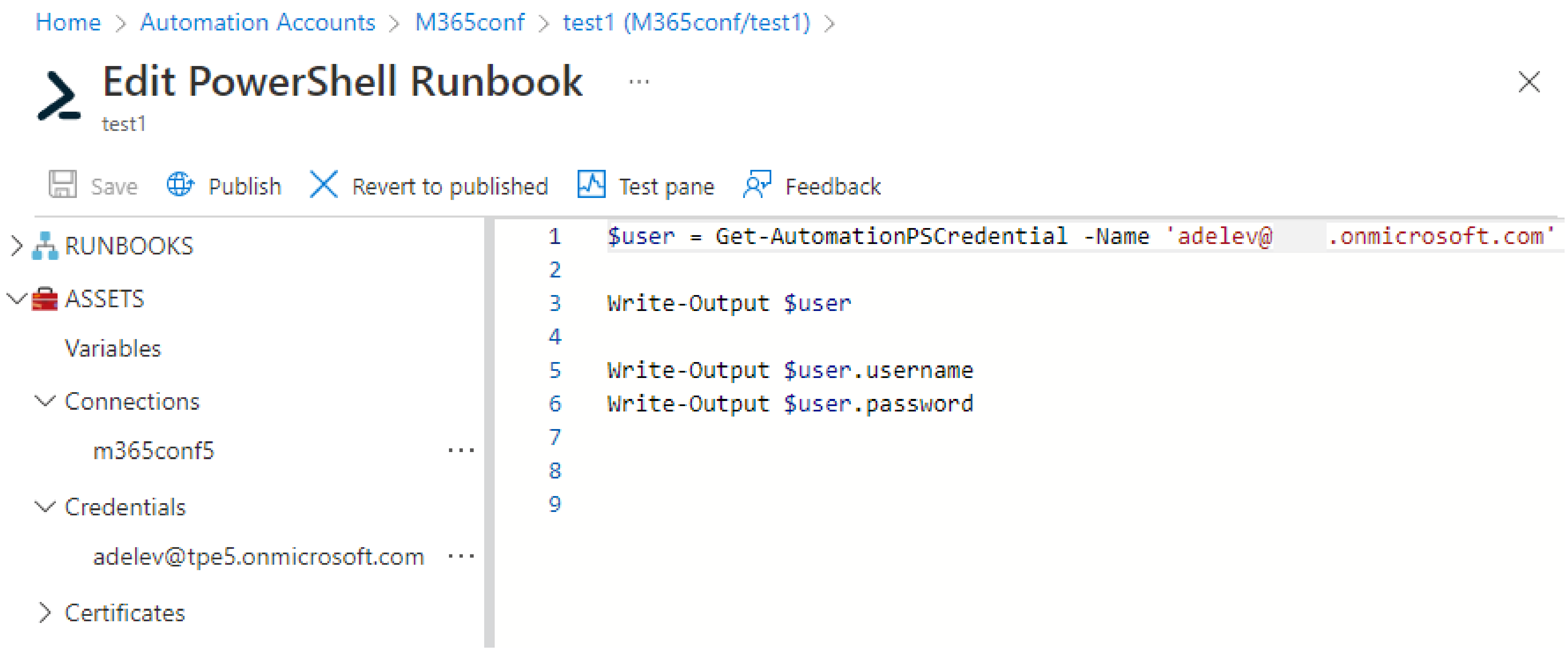
Permissions ⓘ

This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to
can result in failures. Learn more

Automation Accounts Demo

- Migrate your PowerShell scripts to the cloud
- Secure access (Connections, Managed Identity, Key Vault, Firewall)

Access assets in scripts


Home > Automation Accounts > M365conf > test1 (M365conf/test1) >
Edit PowerShell Runbook ...
test1
Save
Publish
Revert to published
Test pane
Feedback
RUNBOOKS
ASSETS
Variables
Connections
m365conf5 ...
Credentials
adelev@tpe5.onmicrosoft.com ...
Certificates

```
$user = Get-AutomationPSCredential -Name 'adelev@    .onmicrosoft.com'

Write-Output $user

Write-Output $user.username
Write-Output $user.password
```

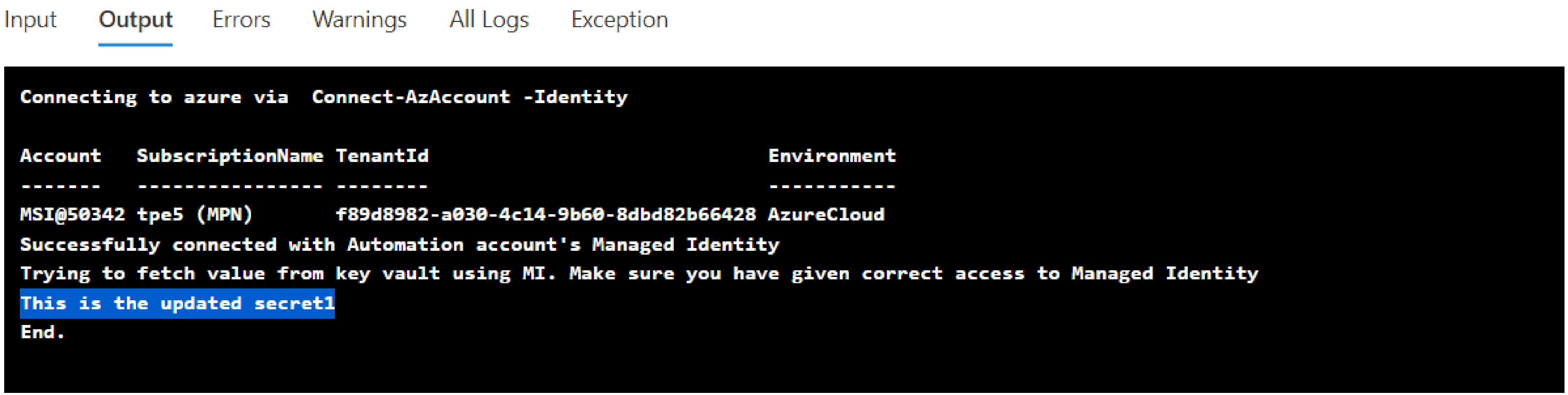
Using a system-assigned managed identity

- The latest version of Az PowerShell modules Az.Accounts, Az.Resources, Az.Automation, Az.KeyVault.
- Using a system-assigned managed identity for an Azure Automation account
- https://docs.microsoft.com/en-us/azure/automation/enable-managed-identity-for-automation

Use a System managed identity and access Key Vault

```
Connect-AzAccount –Identity
```

```
$secret = Get-AzKeyVaultSecret -VaultName 'm365conf’ -
         Name 'secret1'
```



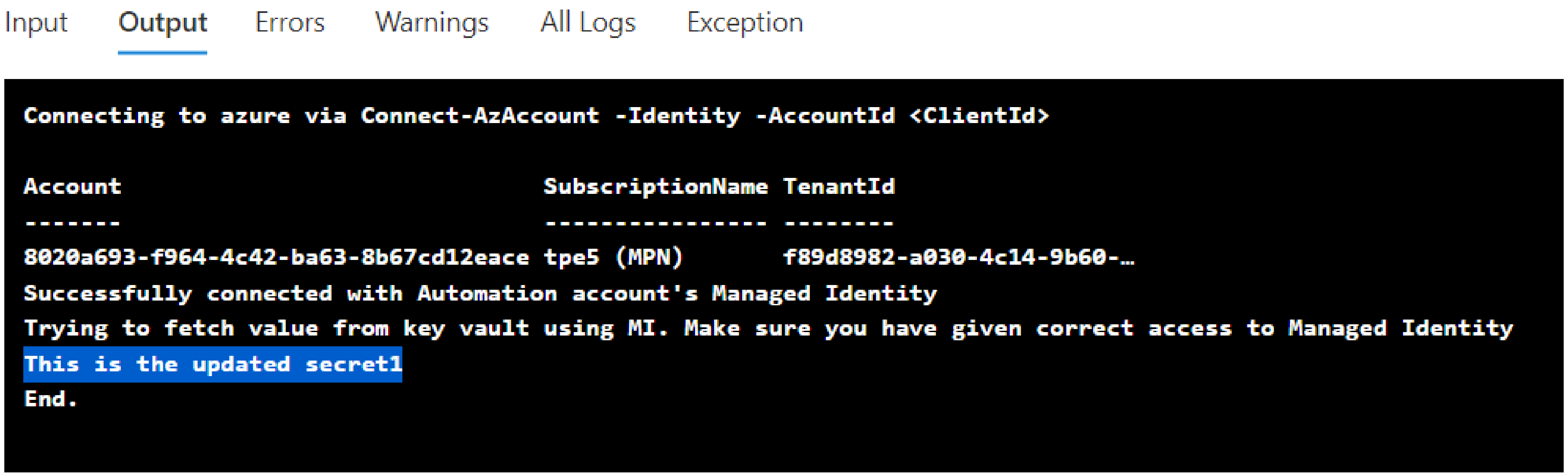
```
Connecting to azure via  Connect-AzAccount -Identity

Account    SubscriptionName TenantId                             Environment
-------    ---------------- --------                             -----------
MSI@50342 tpe5 (MPN)        f89d8982-a030-4c14-9b60-8dbd82b66428 AzureCloud
Successfully connected with Automation account's Managed Identity
Trying to fetch value from key vault using MI. Make sure you have given correct access to Managed Identity
This is the updated secret1
End.
```

Use a User managed identity and access Key Vault

```
Connect-AzAccount -Identity -AccountId "<clientid>“
```

```
$secret = Get-AzKeyVaultSecret -VaultName 'm365conf’
          -Name 'secret1'
```



```
Connecting to azure via Connect-AzAccount -Identity -AccountId <ClientId>

Account                              SubscriptionName TenantId
-------                              ---------------- --------
8020a693-f964-4c42-ba63-8b67cd12eace tpe5 (MPN)       f89d8982-a030-4c14-9b60-…
Successfully connected with Automation account's Managed Identity
Trying to fetch value from key vault using MI. Make sure you have given correct access to Managed Identity
This is the updated secret1
End.
```

Basic Authentication – "This time, we mean it"

- Deprecation of Basic authentication in Exchange Online https://docs.microsoft.com/en-us/lifecycle/announcements/exchange-online-basic-auth-deprecated
- …announcing that, effective October 1, 2022, we will begin to permanently disable Basic Auth in all tenants, regardless of usage, with the exception of SMTP Auth. https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-september-2021-update/ba-p/2772210
- We're removing the ability to use Basic authentication in Exchange Online for Exchange ActiveSync (EAS), POP, IMAP, Remote PowerShell, Exchange Web Services (EWS), Offline Address Book (OAB), Outlook for Windows, and Mac.
- We're also disabling SMTP AUTH in all tenants in which it's not being used. (Fall 2021)

Create a self-signed certificate with PS

```powershell
# Certificate (PFX)
$cert = New-SelfSignedCertificate `
    -NotAfter $(Get-Date).AddYears($certYears) `
    -Type SSLServerAuthentication `
    -FriendlyName 'MyAuthCert' `
    -Subject 'CN=MyCompany' `
    -CertStoreLocation 'Cert:\CurrentUser\My' `
    -KeySpec KeyExchange
```

Azure Logic Apps

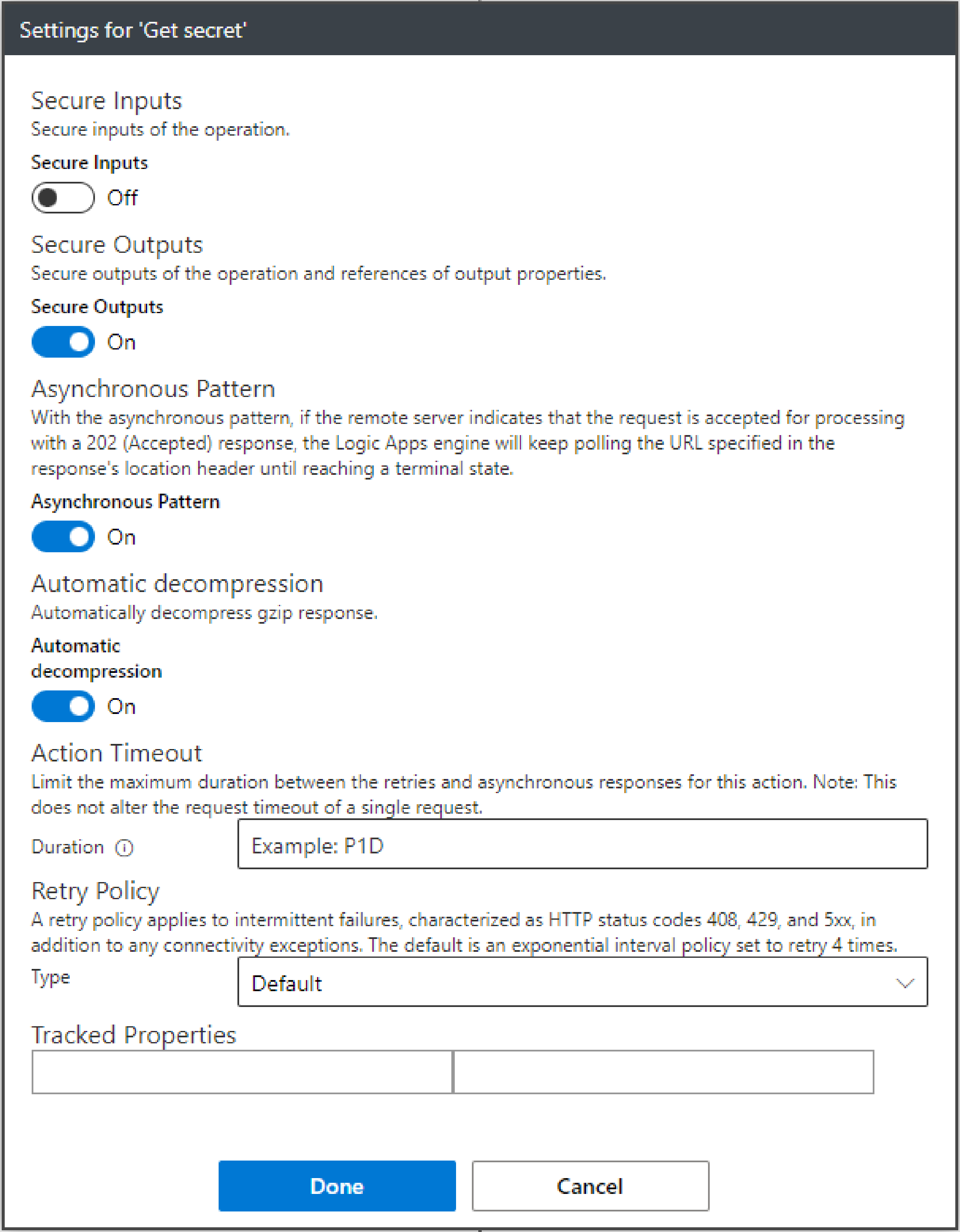
- Perfect for (small) business processes
- Secure connections

Azure Logic Apps

Tip:

Use Secure Outputs

(Logging)



Settings for 'Get secret'

Secure Inputs

Secure inputs of the operation.

Secure Inputs

Off

Secure Outputs

Secure outputs of the operation and references of output properties.

Secure Outputs

On

Asynchronous Pattern

With the asynchronous pattern, if the remote server indicates that the request is accepted for processing with a 202 (Accepted) response, the Logic Apps engine will keep polling the URL specified in the response's location header until reaching a terminal state.

Asynchronous Pattern

On

Automatic decompression

Automatically decompress gzip response.

Automatic decompression

On

Action Timeout

Limit the maximum duration between the retries and asynchronous responses for this action. Note: This does not alter the request timeout of a single request.

Duration ⓘ Example: P1D

Retry Policy

A retry policy applies to intermittent failures, characterized as HTTP status codes 408, 429, and 5xx, in addition to any connectivity exceptions. The default is an exponential interval policy set to retry 4 times.

Type Default

Tracked Properties

App Services

- Web sites
- Web jobs
- Azure Functions

Azure Web App Sandbox – Security Concepts

- **Security/Isolation:** Running in a sandbox (isolating its execution from other instances)
- **Sandbox:** Sandbox guarantees a minimum level of service, but has with runtime limits as well (so that an app can not disrupt other concurrently-executing apps on the same machine)
- **Includes** all Azure Web Apps (as well as Mobile App/Services, WebJobs and Functions)
- **Lifetime:** Begins with the creation of this IIS w3wp.exe process, followed by php-cgi.exe or node.exe, CSC.EXE, etc. (memory allocated by php-cgi.exe and w3wp.exe both count towards the same memory quota.)
- https://github.com/projectkudu/kudu/wiki/Azure-Web-App-sandbox

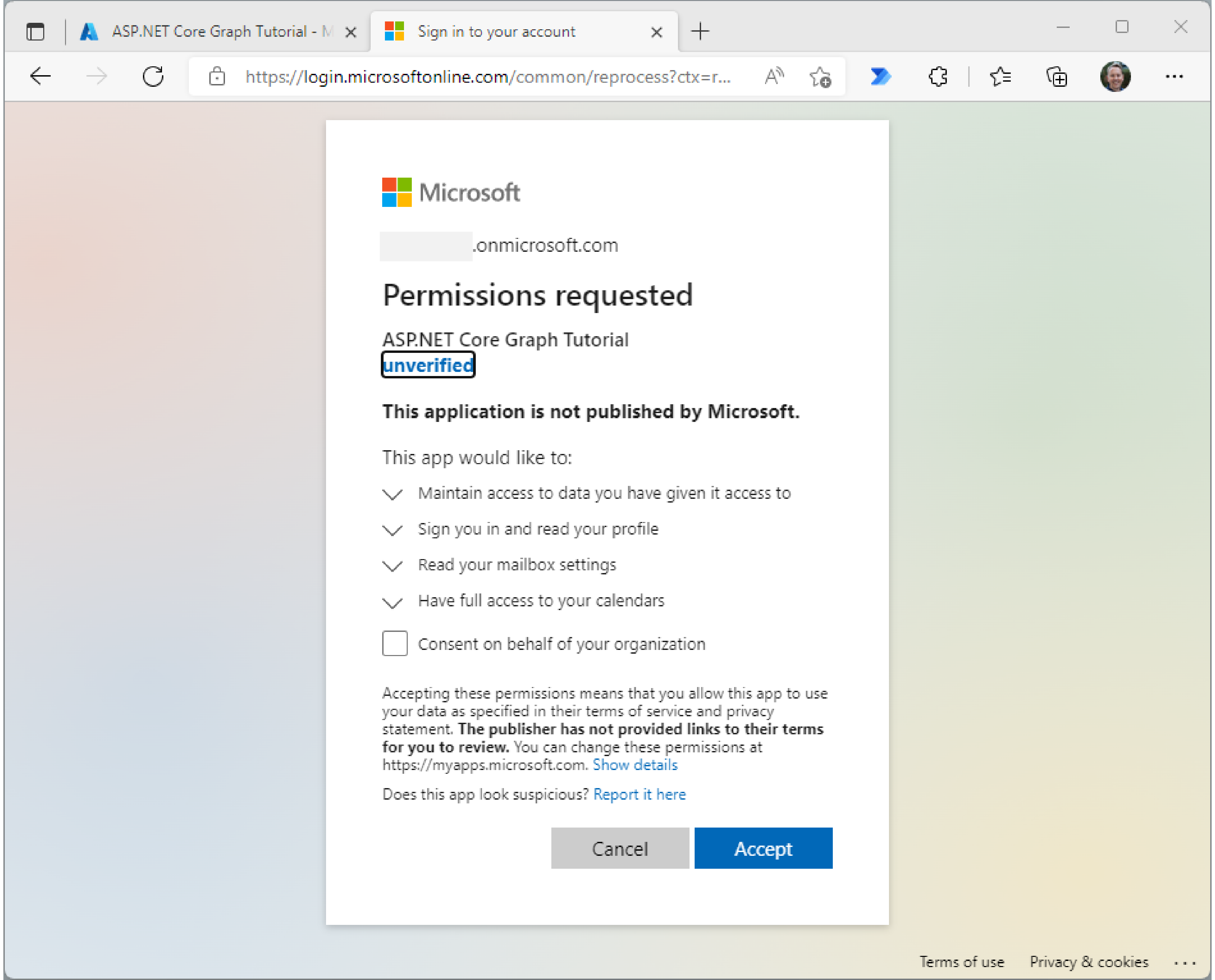
Access Key Vault from App config settings

```
@Microsoft.KeyVault(SecretUri=https://
m365conf.vault.azure.net/secrets/secret1/)
```

https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

Integrate MSAL into your (web) apps

- https://docs.microsoft.com/en-us/graph/tutorials/aspnet-core
- https://github.com/microsoftgraph/msgraph-training-aspnet-core


ASP.NET Core Graph Tutorial - M
Sign in to your account
https://login.microsoftonline.com/common/reprocess?ctx=r...
Microsoft

[redacted].onmicrosoft.com

Permissions requested

ASP.NET Core Graph Tutorial
unverified

This application is not published by Microsoft.

This app would like to:

- Maintain access to data you have given it access to
- Sign you in and read your profile
- Read your mailbox settings
- Have full access to your calendars

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Summary
Secure your Enterprise applications with Azure

- Identify your use cases
- Use built-in services & Azure Advisor
- See, if PaaS is an option
- Secure services with
- Apps (Managed Identities, Certificates, …)
- Key Vault for secrets

Microsoft 365 CONFERENCE

Microsoft Viva
Microsoft Teams
Microsoft SharePoint
Microsoft Power Platform

CO PRODUCED BY MICROSOFT AND M365 CONFERENCE

Thank you!

Connect with me!
@atwork
https://github.com/tonipohl

FOR INFORMATION ABOUT OUR NEXT IN PERSON EVENT, VISIT OUR WEBSITE AT

M365Conf.com

Microsoft 365 CONFERENCE

Microsoft Viva
Microsoft Teams
Microsoft SharePoint
Microsoft Power Platform

CO PRODUCED BY MICROSOFT AND M365 CONFERENCE