Secure your Enterprise applications with Azure

Martina Grom
Azure & Microsoft 365 MVP, Microsoft RD, CEO atwork
@magrom | martina.grom@atwork.at | www.atwork-it.com

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

#GLOBALAZURE 2022
BY COMMUNITY • FOR COMMUNITY •

@magrom @atwork

Moving workloads and data to the cloud?

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

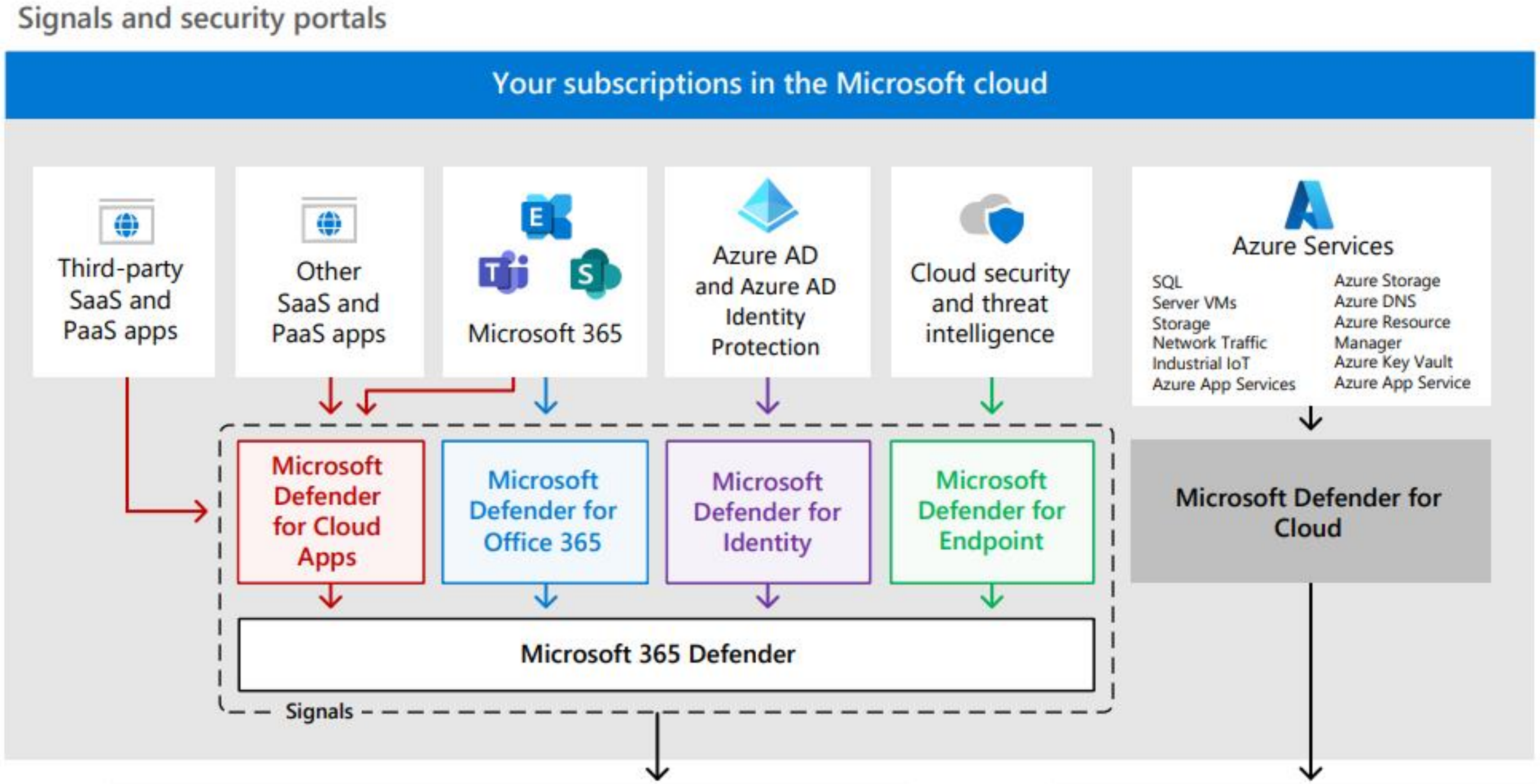
Consultant: “Azure is secure by default.”

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/

Components and relationships



Signals and security portals

Your subscriptions in the Microsoft cloud

Third-party SaaS and PaaS apps

Other SaaS and PaaS apps

Microsoft 365

Azure AD and Azure AD Identity Protection

Cloud security and threat intelligence

Azure Services

SQL
Server VMs
Storage
Network Traffic
Industrial IoT
Azure App Services

Azure Storage
Azure DNS
Azure Resource Manager
Azure Key Vault
Azure App Service

Microsoft Defender for Cloud Apps

Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Defender for Endpoint

Microsoft Defender for Cloud

Microsoft 365 Defender

Signals

Microsoft 365 Defender portal

Signals from sign-ins, Windows 11 or 10 desktops, and Office 365 and other cloud apps feed into the components of Microsoft 365 Defender.

The Microsoft 365 Defender portal shows the aggregate security posture and details of incidents and alerts.

Azure Security Center

Signals from Azure services feed into Microsoft Defender for Cloud.

The Azure Security Center shows the aggregate security posture and details of incidents and alerts.

Identify your use cases!

IaaS

PaaS

SaaS

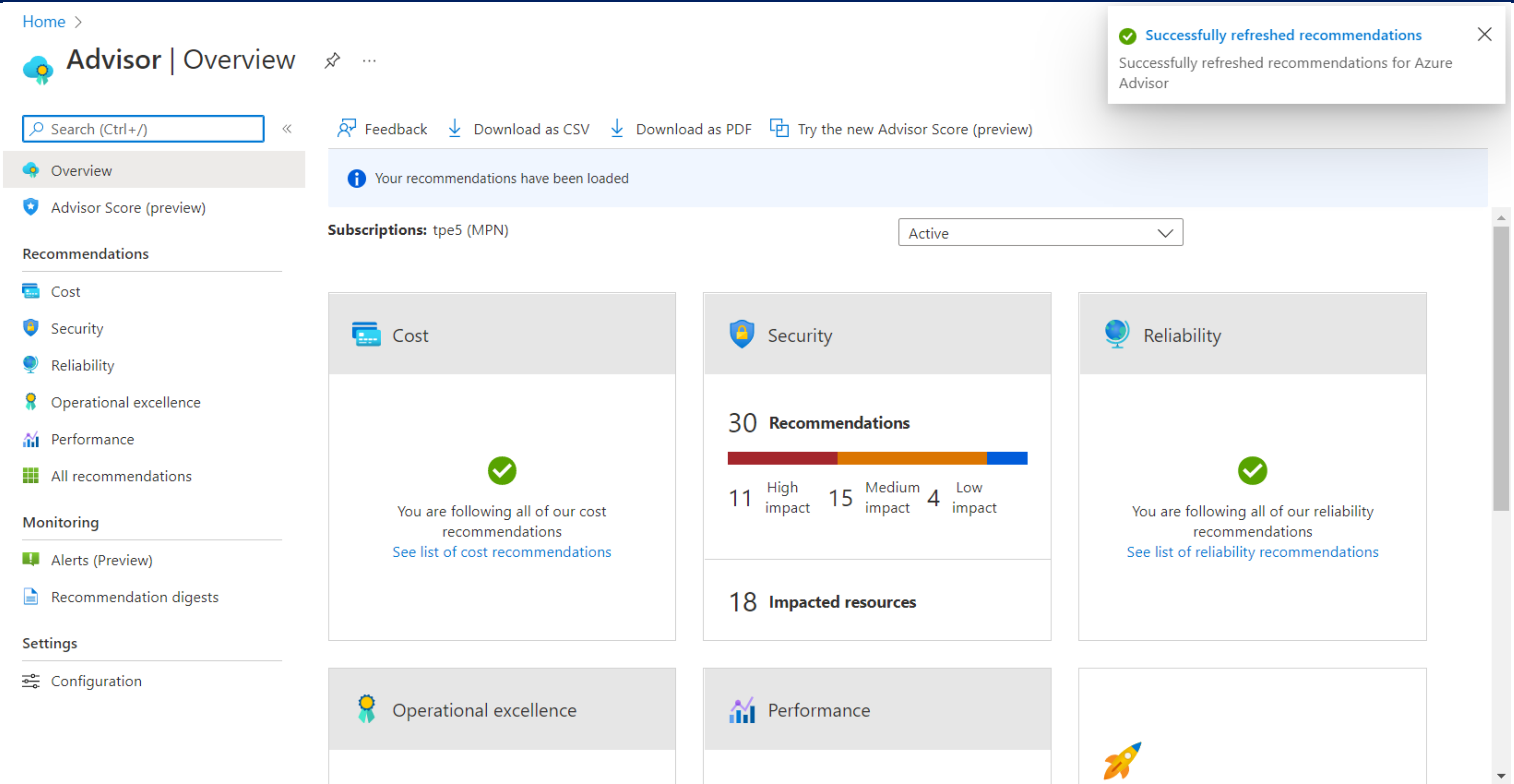
Typical workloads types

- VM´s (Lift & Shift)
- (Web) Apps
- PowerShell Scripts
- Business workflows

How to secure your resources

- Tip: Use Azure Advisor
- This tool is helpful (and you can create exempts)

Tip: Use Azure Advisor



Advisor | Overview

Successfully refreshed recommendations

Successfully refreshed recommendations for Azure Advisor

Your recommendations have been loaded

Subscriptions: tpe5 (MPN)

You are following all of our cost recommendations

30 **Recommendations**

11 High impact 15 Medium impact 4 Low impact

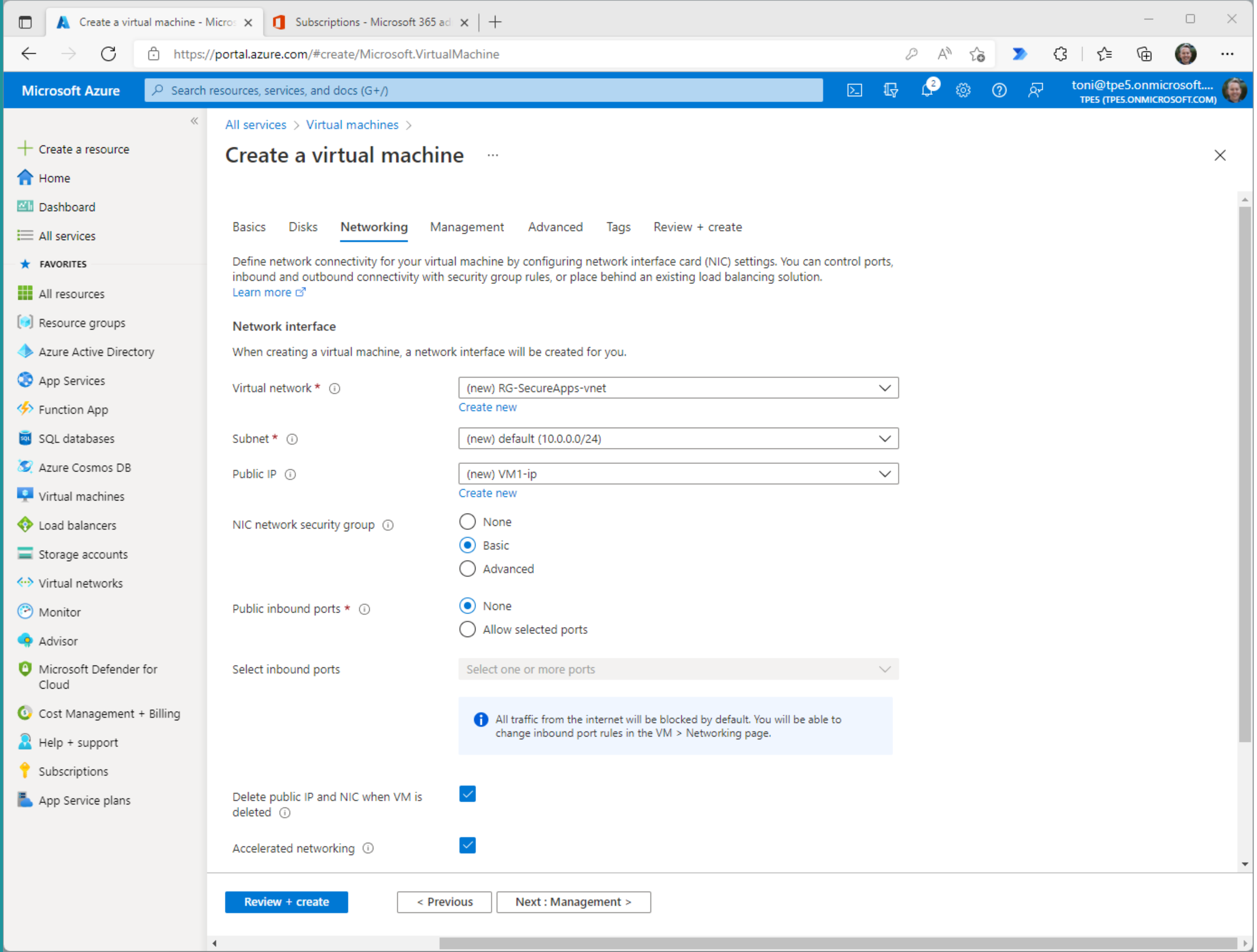
18 **Impacted resources**

You are following all of our reliability recommendations

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

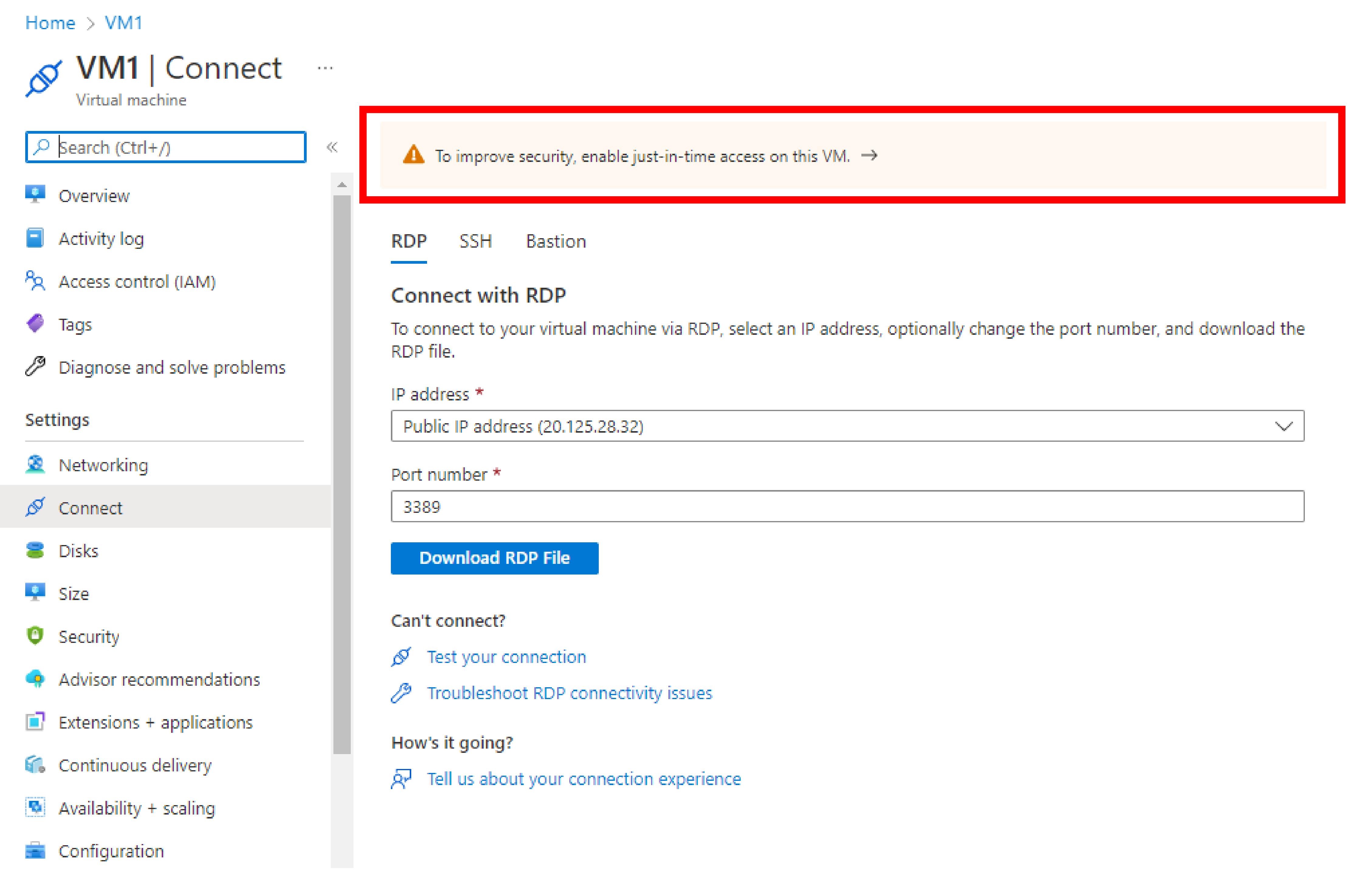
Select inbound ports: Select one or more ports

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



⚠ 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.

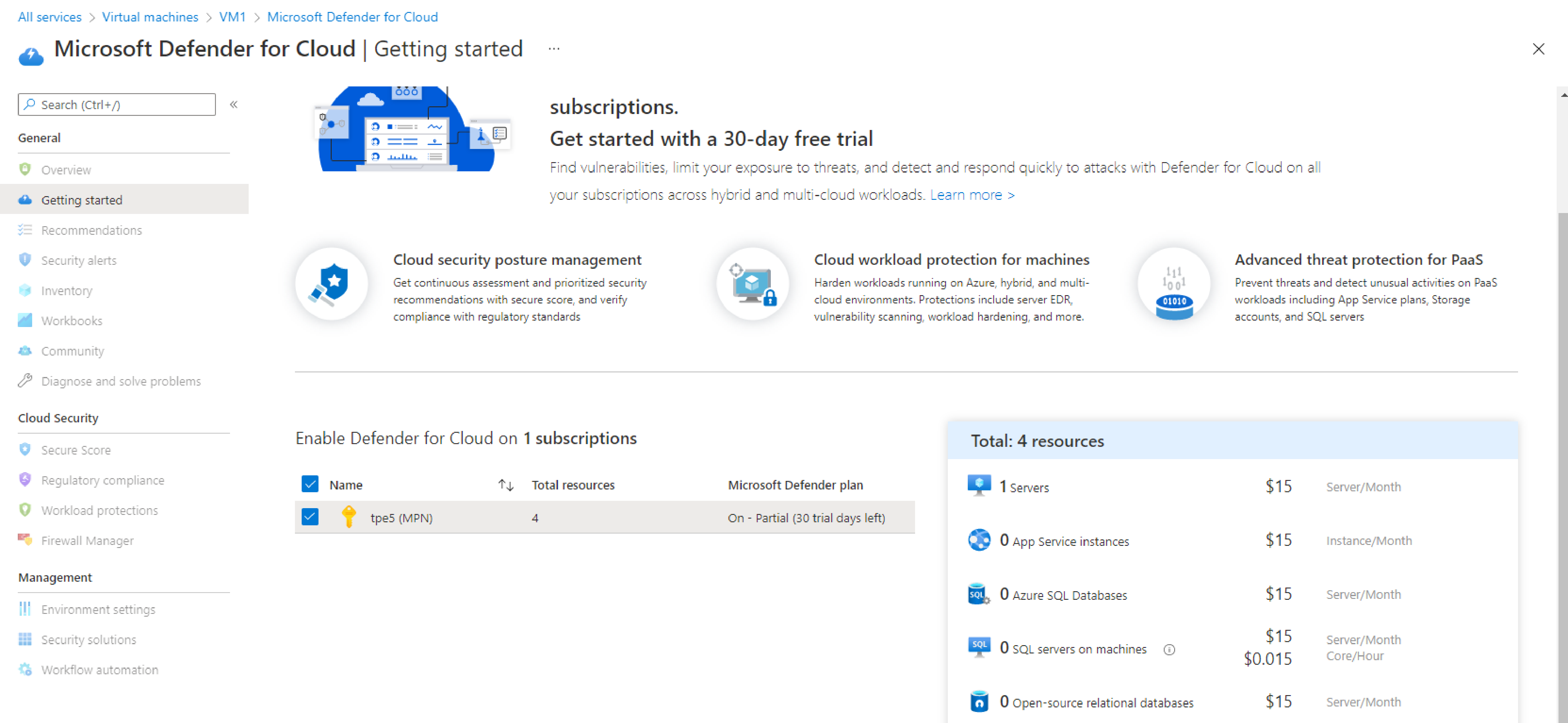
IP address *: Public IP address (20.125.28.32)

Port number *: 3389

Can't connect?

How's it going?

JIT requires 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

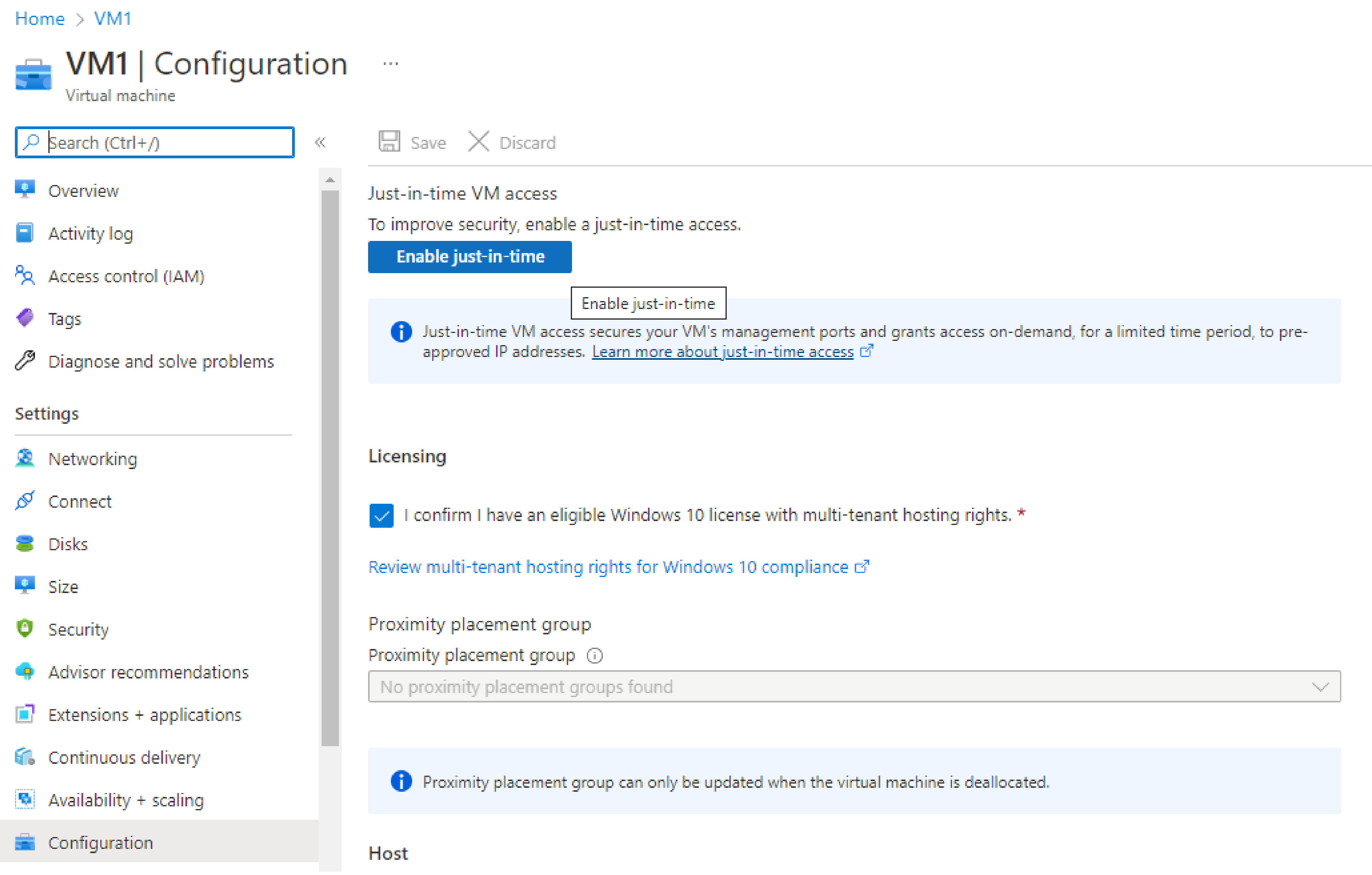
Enable Defender for Cloud on **1 subscriptions**

☑ 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

To improve security, enable a just-in-time access.

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

Licensing

☑ I confirm I have an eligible Windows 10 license with multi-tenant hosting rights. *

Review multi-tenant hosting rights for Windows 10 compliance

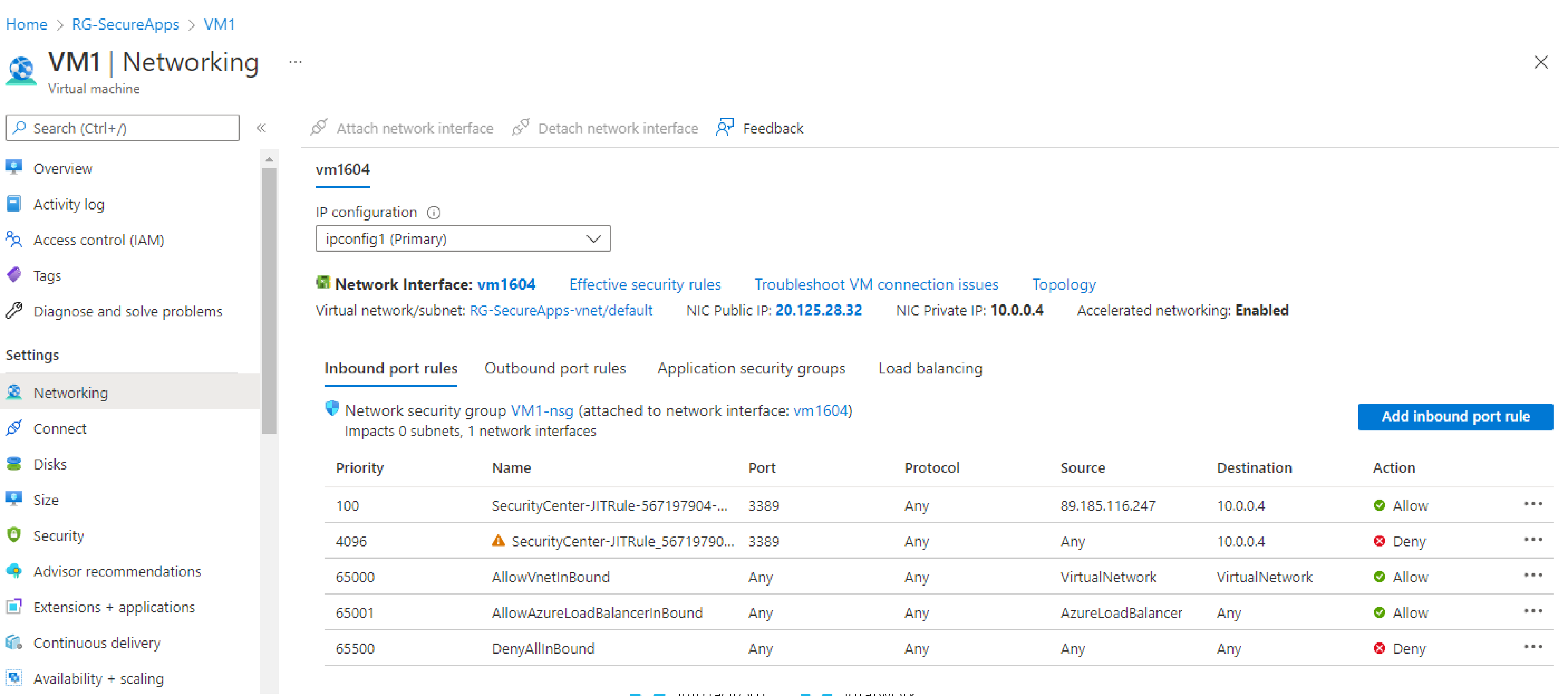
Proximity placement group

Proximity placement group: No proximity placement groups found

Proximity placement group can only be updated when the virtual machine is deallocated.

Host

JIT creates a temporary rule in the Firewall



Home > RG-SecureApps > VM1

VM1 | Networking

Virtual machine

IP configuration: ipconfig1 (Primary)

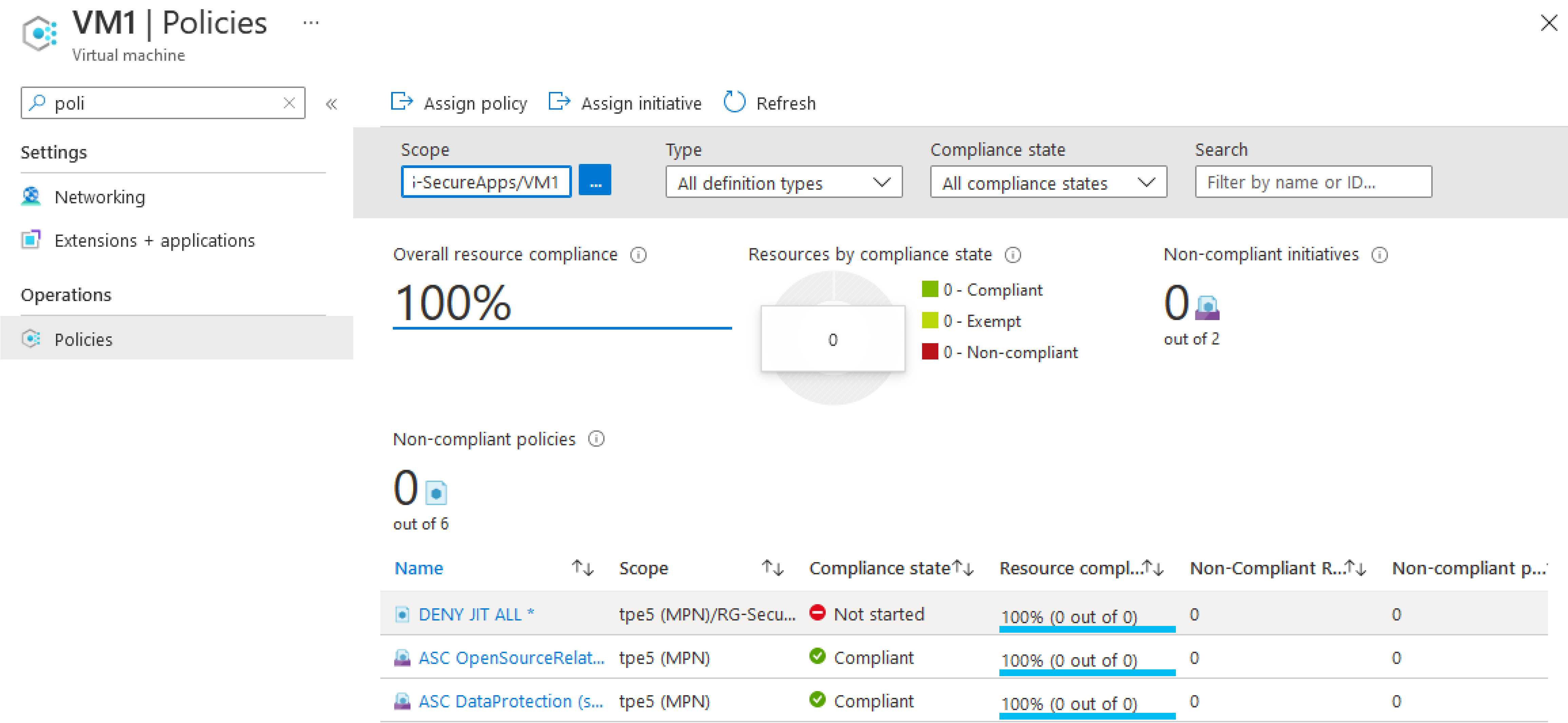
Network Interface: vm1604 Effective security rules Troubleshoot VM connection issues Topology

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

Enforce JIT with a policy



VM1 | Policies

Virtual machine

Scope: i-SecureApps/VM1

Type: All definition types

Compliance state: All compliance states

Search: Filter by name or ID...

Overall resource compliance: 100%

Resources by compliance state: 0

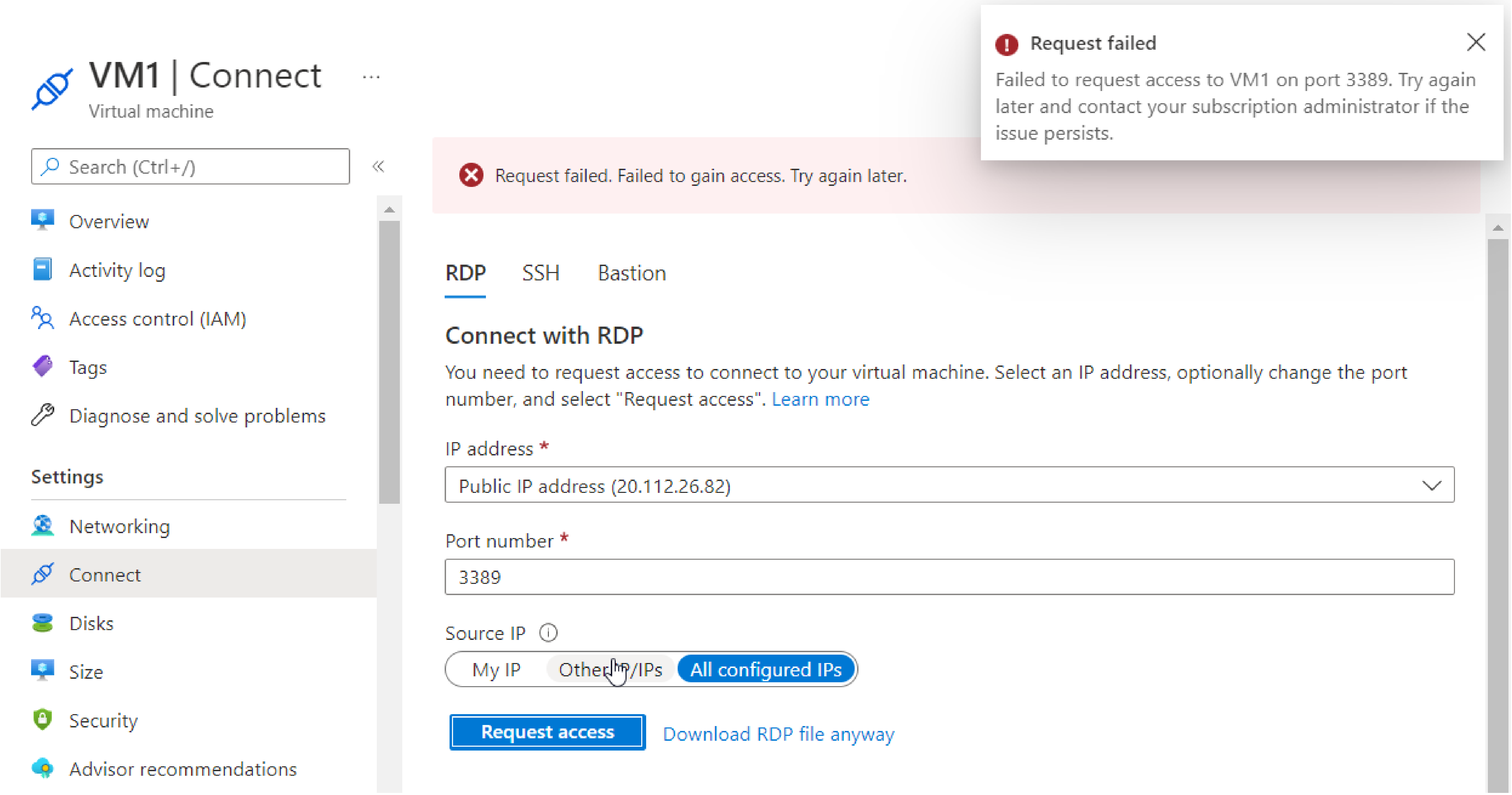
- 🟩 0 - Compliant
- 🟩 0 - Exempt
- 🟥 0 - Non-compliant

Non-compliant initiatives: 0 out of 2

Non-compliant policies: 0 out of 6

Name	Scope	Compliance state	Resource compl...	Non-Compliant R...	Non-compliant p...
DENY JIT ALL *	tpe5 (MPN)/RG-Secu...	Not started	100% (0 out of 0)	0	0
ASC OpenSourceRelat...	tpe5 (MPN)	Compliant	100% (0 out of 0)	0	0
ASC DataProtection (s...	tpe5 (MPN)	Compliant	100% (0 out of 0)	0	0

Policy in action



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

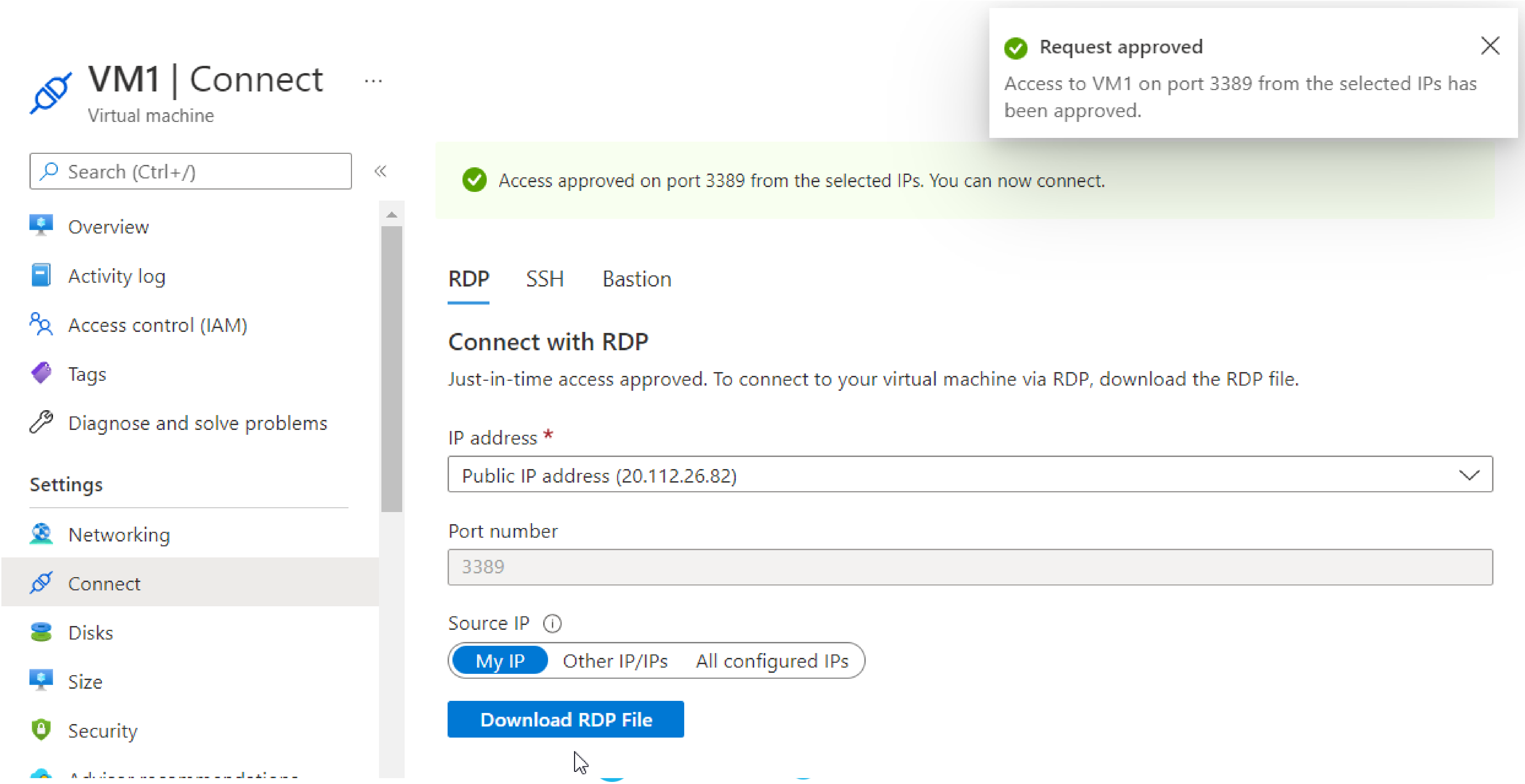
You need to request access to connect to your virtual machine. Select an IP address, optionally change the port number, and select "Request access". Learn more

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



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

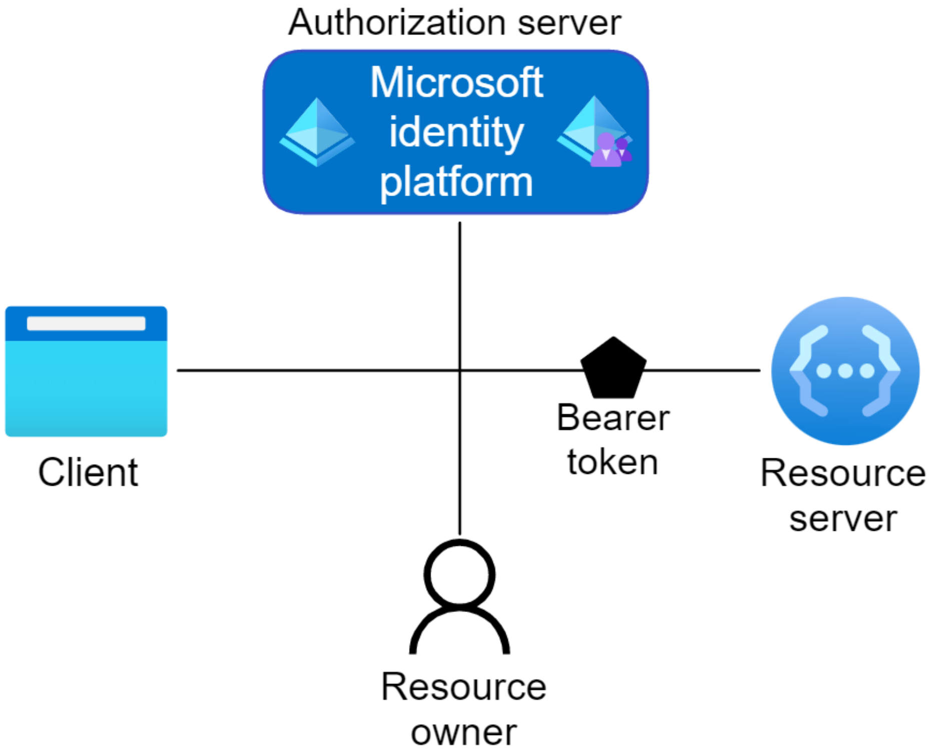
Source IP: [✓ My IP] Other IP/IPs All configured IPs

Securing access

- In M365/Azure, the basis is identity…

“Modern Authentication”

“The Microsoft identity platform implements the OAuth 2.0 authorization protocol. OAuth 2.0 is a method through which a third-party app can access web-hosted resources on behalf of a user.”



Apps Demo

- Access resources with specific permissions
- For development purposes, use jwt.ms

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 Name 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. Automatically created 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

Azure Logic Apps

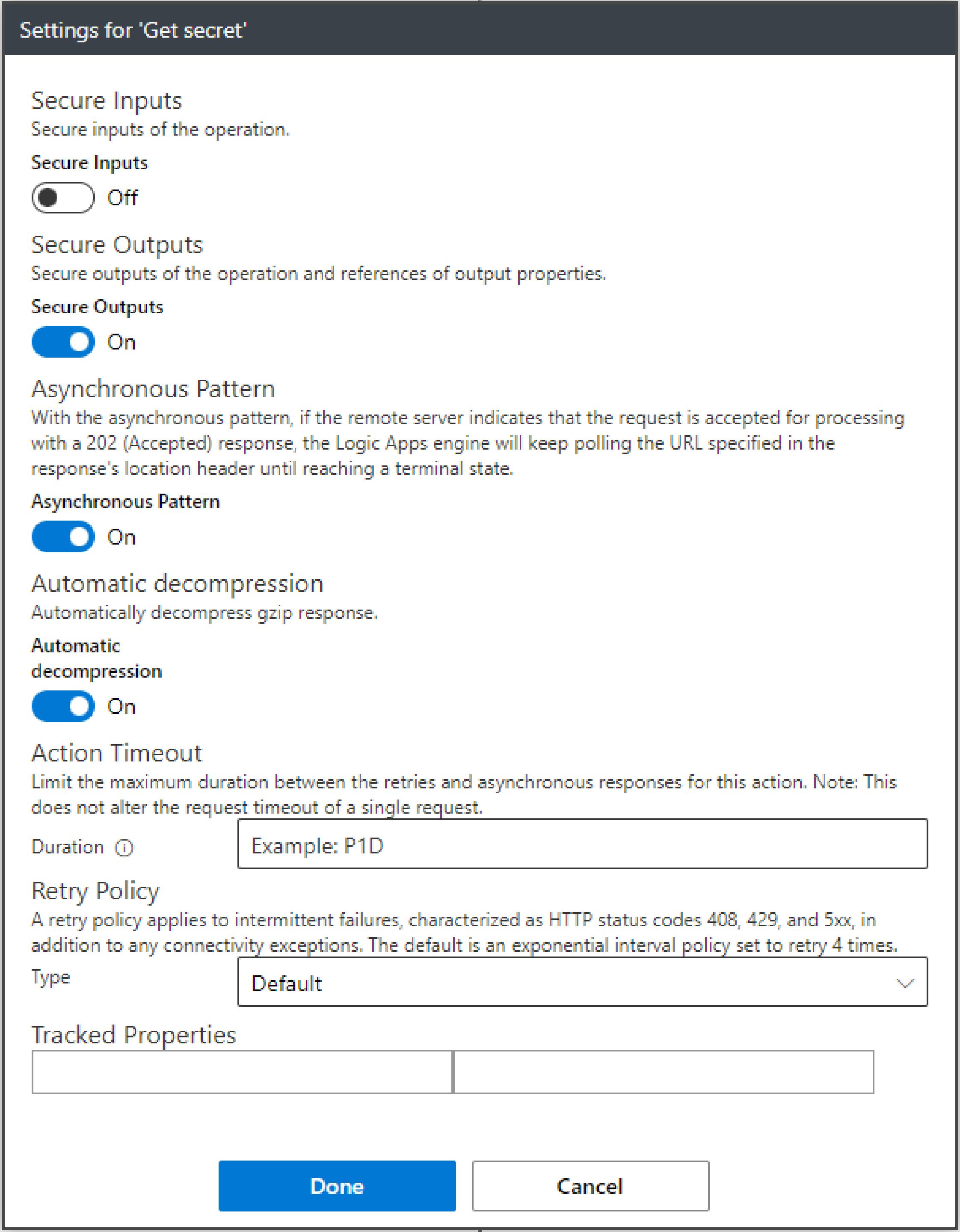
- Perfect for no/low code business processes
- Secure connections + Managed Identity + KeyVault

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

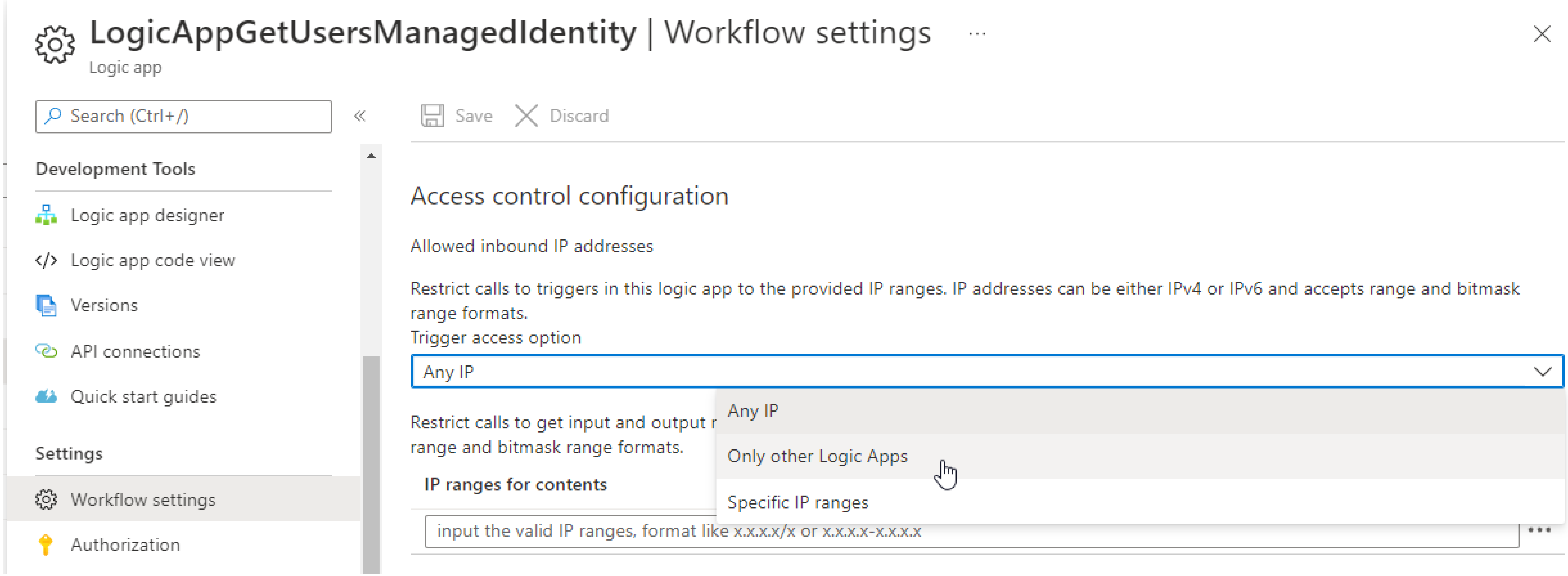
Retry Policy

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

Azure Logic Apps: Secure the trigger



LogicAppGetUsersManagedIdentity | Workflow settings

Logic app

Access control configuration

Allowed inbound IP addresses

Restrict calls to triggers in this logic app to the provided IP ranges. IP addresses can be either IPv4 or IPv6 and accepts range and bitmask range formats.

Trigger access option

Any IP

- Any IP
- Only other Logic Apps
- Specific IP ranges

Restrict calls to get input and output r

range and bitmask range formats.

IP ranges for contents

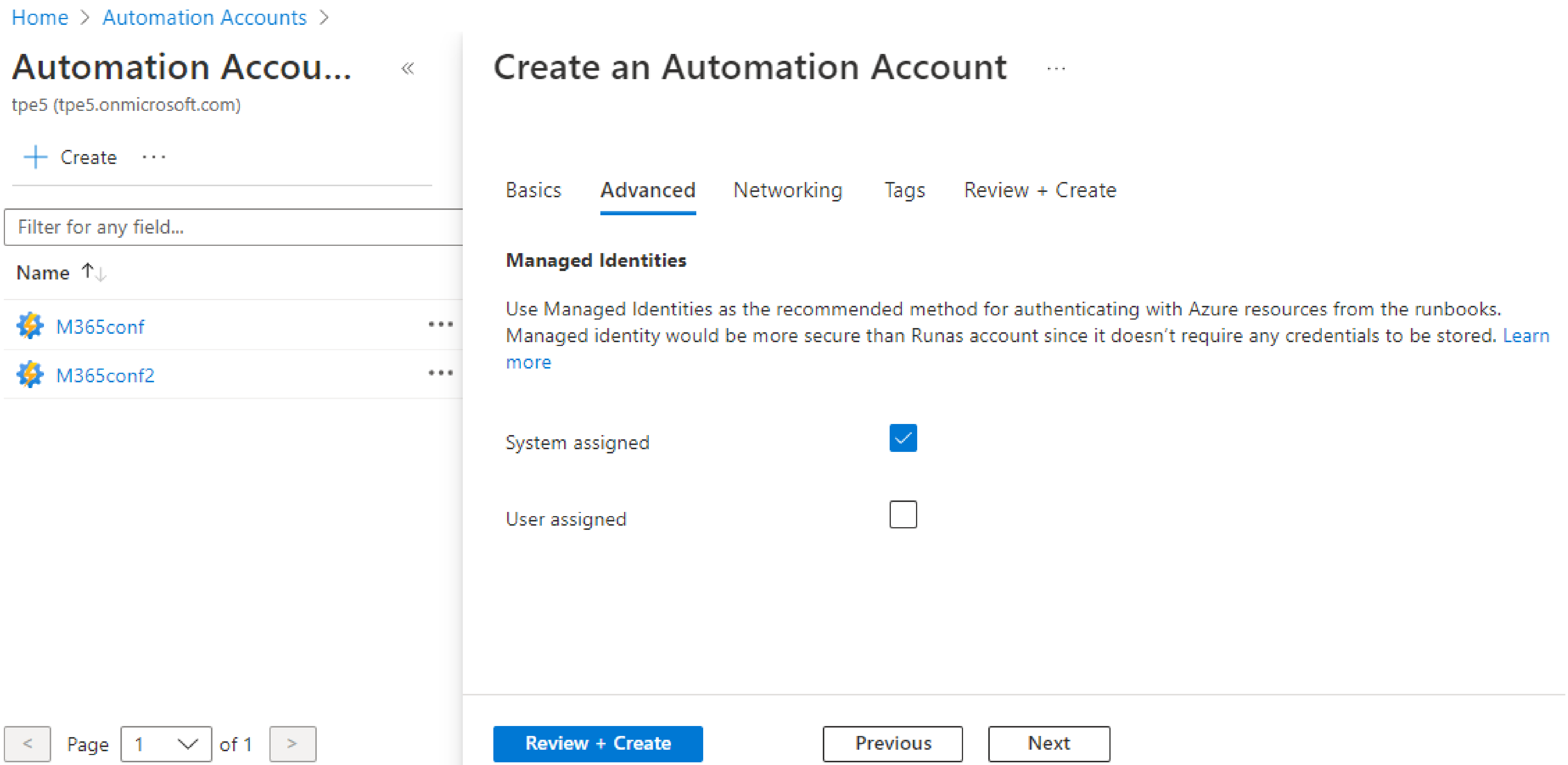
input the valid IP ranges, format like x.x.x.x/x or x.x.x.x-x.x.x.x

@magrom @atwork

Automation Accounts Demo

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

Automation Accounts are for scripts



Home > Automation Accounts >

Automation Accou...

tpe5 (tpe5.onmicrosoft.com)

M365conf

M365conf2

Create an Automation Account

Managed Identities

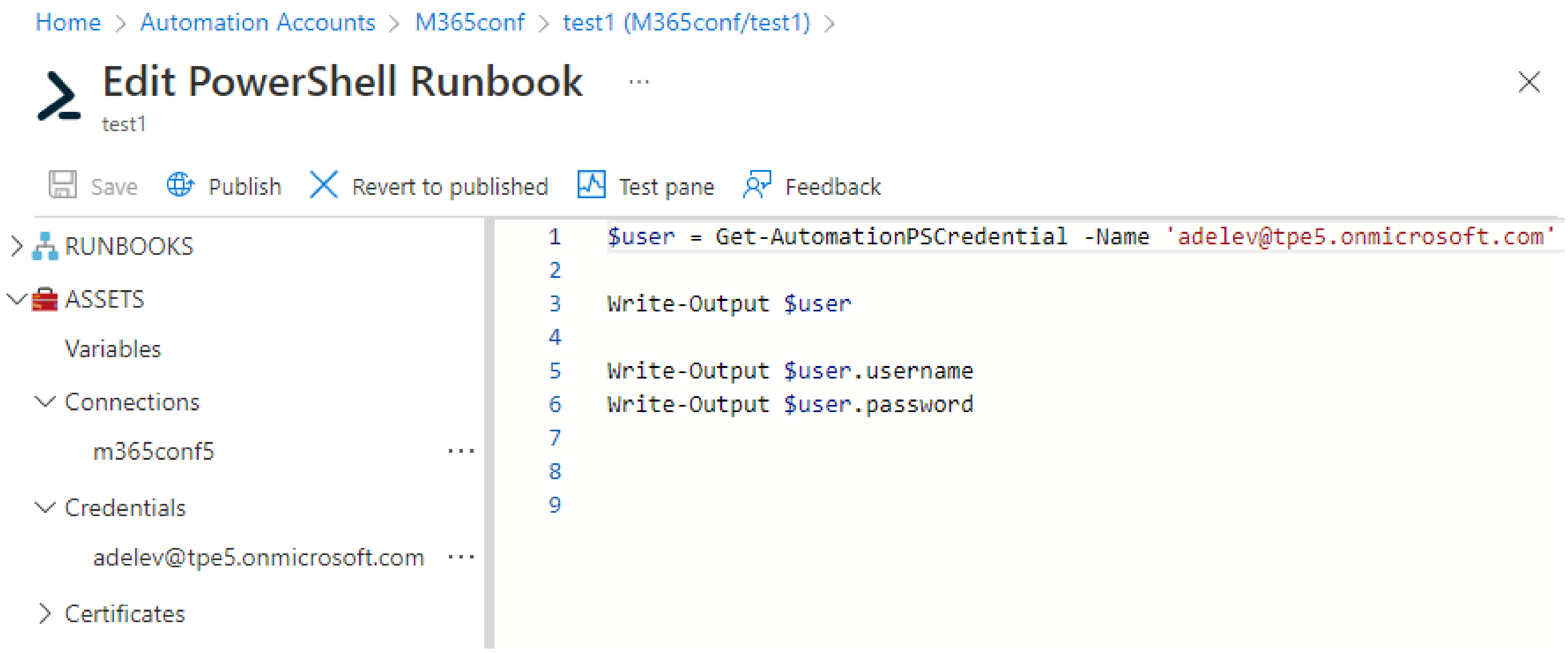
Use Managed Identities as the recommended method for authenticating with Azure resources from the runbooks. Managed identity would be more secure than Runas account since it doesn't require any credentials to be stored. Learn more

System assigned ☑

User assigned □

@magrom @atwork

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@tpe5.onmicrosoft.com'

Write-Output $user

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

@magrom @atwork

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

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

@magrom @atwork

App Services

- Web sites
- Web jobs
- Azure Functions

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

Logging + Monitoring

… should be part of every app or solution

Secure your Enterprise applications with Azure

- Identify your use cases
- Use built-in services & Azure Advisor
- Always consider PaaS
- Apps (Managed Identities, Certificates, …)
- Key Vault for secrets
- Use built-in functionality (Connections…)
- Logging & Monitoring

Thank you!

Check out samples and links on my GitHub repo
https://github.com/tonipohl/SecureAppsWithAzure

https://virtual.globalazure.net/
https://globalazure.at/

@magrom @atwork