

# What's new in Azure Infrastructure

- Jesper Fütterer Bing
- Azure MVP
- Cloud Architect, APENTO
- @jefutte



# Agenda

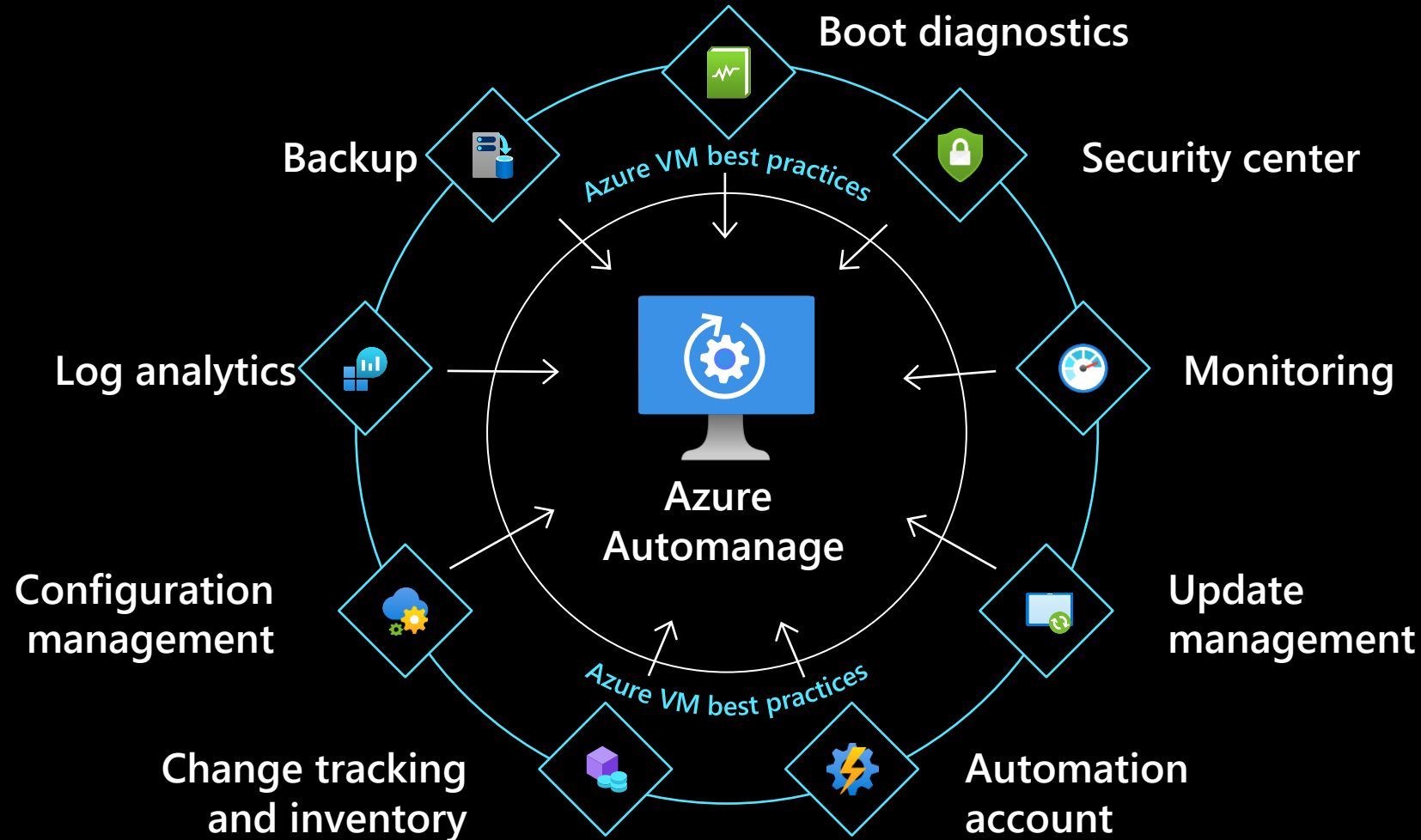
- Compute
- Networking
- Storage
- Management



# Azure Automanage - GA



# Intelligently onboard to select Azure services



# Managed through profiles

Define profiles centrally, and assign automatical with Azure Policy

The screenshot displays the Azure Arc Automanage console for a server named 'arc04'. The interface is divided into a left-hand navigation pane, a central main content area, and a right-hand 'Configuration profile details' pane.

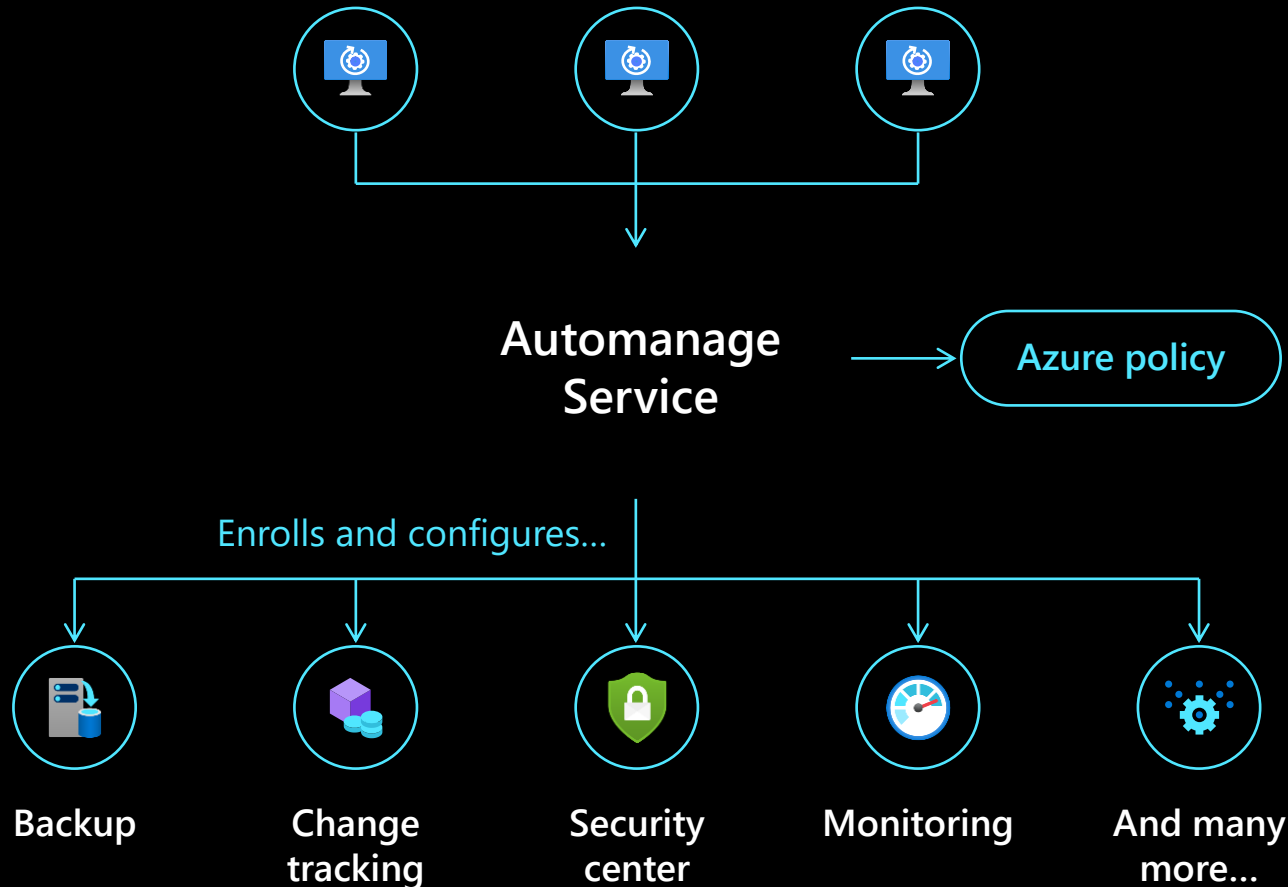
**Left Navigation Pane:** Includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Connect (preview), Windows Admin Center (preview), Security, Extensions, Properties, Locks), Operations (Policies, Machine Configuration, Automanage, Updates, Inventory, Change tracking), Monitoring (Insights, Logs), Automation (Tasks (preview)), and Support + troubleshooting.

**Main Content Area:** The title bar shows 'Home > arc04 > arc04 | Automanage'. Below the title bar, there are links for 'Manage multiple machines', 'Refresh', and 'Give feedback'. A descriptive paragraph states: 'Automanage machine best practices simplifies your management experience by automatically onboarding, configuring, and monitoring your machines to comply with the selected configuration profile. If any service or setting drifts from the desired configuration, Automanage will auto-remediate the service to ensure it is conformant to the configuration profile selected. [Learn more](#)'. Under 'Configuration profile', three options are listed: 'Azure best practices: Production' (Recommended for production environments, includes insights and backup), 'Azure best practices: Dev / Test' (Best for dev/test environments where robust backup and monitoring are not necessary), and 'Custom profile' (Selected; Onboard your machines with custom settings and enable or disable any of the services. [View Azure best practices profiles](#)). Below this, a 'Custom profile' dropdown menu is set to 'Cloudpuzzles-Arc-Machines [westeurope]', with links for 'Create new' and 'View profile details'. An 'Enable' button is at the bottom.

**Right Panel: Configuration profile details**  
Automanage - Azure machine best practices

- Not supported for Azure Arc machines - [Learn more](#)**
- Enable Backup: Off
- Microsoft Antimalware**
- Not supported for Linux and Windows 10 machines - [Learn more](#)**
- Enable Microsoft Antimalware: On
- Enable real-time protection: On
- Enable run a scheduled scan: On
- Scan type: Quick
- Scan day: Saturday
- Scan time: 120
- Machines Insights Monitoring**
- Enable Machines Insights Monitoring: Off
- Automanage Machine Configuration**
- Baseline is not supported for Windows 10 machines - [Learn more](#)**
- Enable Automanage Machine Configuration: Off
- Update Management**
- Not supported for Windows 10 machines - [Learn more](#)**
- Enable Update Management: Off
- Change Tracking and Inventory**
- Enable Change Tracking and Inventory: On
- Microsoft Defender for Cloud**

# Architecture view of Azure Automanage



## HOW IT WORKS

1.

Users enable Automanage with set of parameters

2.

Automanage service calls each service and configures with correct settings

3.

Automanage creates policies

4.

Automanage monitors the policies on a regular cadence

5.

If drift is detected, Automanage brings the VM/associated resource back into the desired state



Generally available

# Windows Admin Center in the Azure portal

Administration of Windows Server VMs with a familiar UI, from the Azure portal



# Windows Admin Center

## Tools

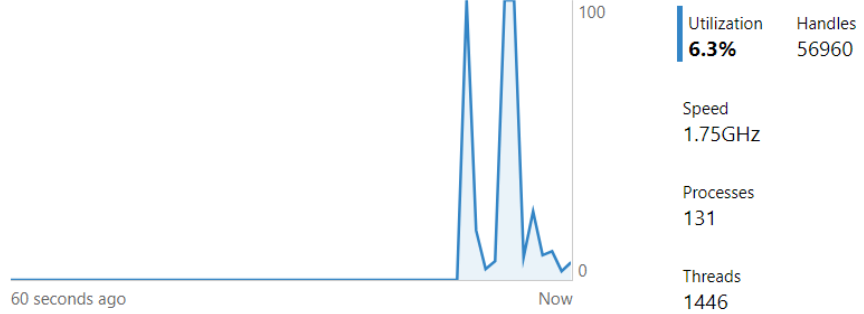
- Search Tools
- Overview
  - Certificates
  - Devices
  - Events
  - Files & file sharing
  - Firewall
  - Installed apps
  - Local users & groups
  - Packet monitoring
  - Performance Monitor
  - PowerShell
  - Processes
  - Registry
  - Remote Desktop
  - Roles & features
  - Scheduled tasks
  - Security
  - Services
  - Storage
  - Updates
  - Settings

## Overview

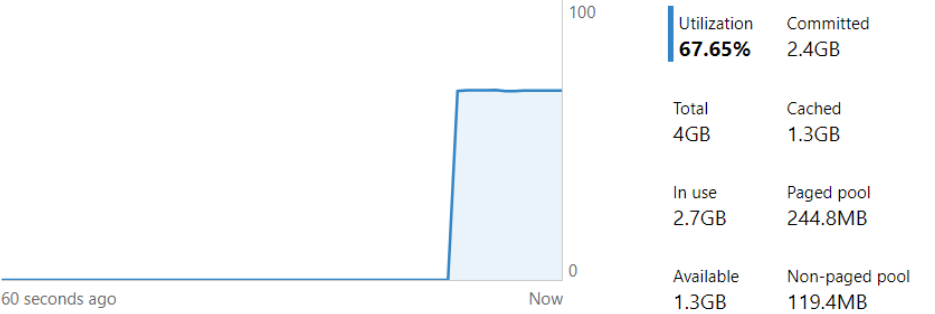
Connect ⌵ 🔄 Enable Disk Metrics 🔄 Refresh

Computer name arc04	Domain WORKGROUP (Workgroup computer)	Operating system Microsoft Windows Server 2022 Datacenter	Version 10.0.20348	Installed memory (RAM) 4 GB
Disk space (Free / Total) 22.37 GB / 44.08 GB	Processors 11th Gen Intel(R) Core(TM) i5-1145G7 @ 2.60GHz	Manufacturer Microsoft Corporation	Logical processors 1	NIC(s) 1
Up time 12:18:47:43	Logged in users 1	Microsoft Defender Antivirus Real-time protection: On	Model Virtual Machine	Windows Defender Application Control (WDAC) Not Enforced

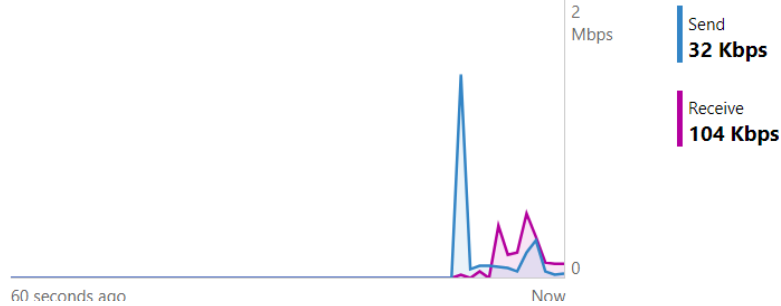
### CPU



### Memory



### Ethernet (Ethernet)





# Manage from everywhere

[Home](#) > [arc04](#) | [Windows Admin Center \(preview\)](#) >



Windows Admin Center ...

## Tools



Overview



Certificates



Devices



Events



Files & file sharing



Firewall



Installed apps



Local users & groups



Packet monitoring



Performance Monitor



PowerShell

## PowerShell

[×](#) Disconnect

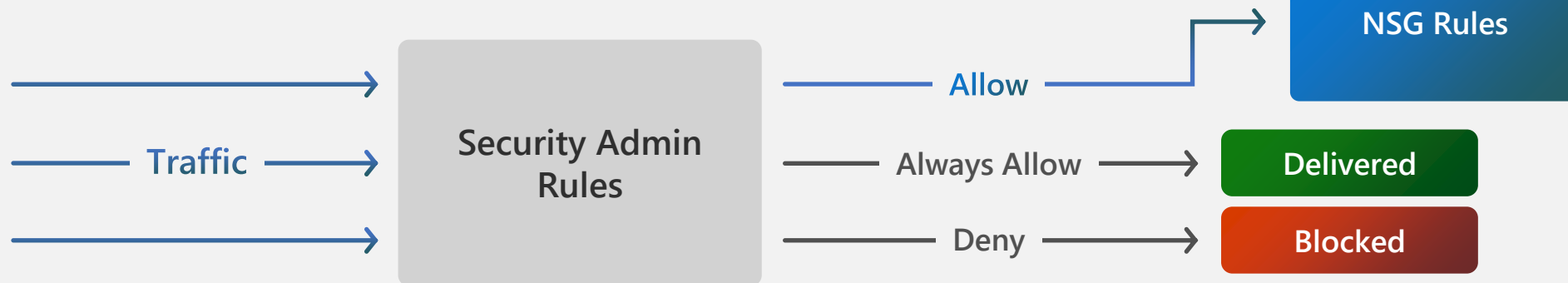
```
Connecting to arc04.  
Username: administrator  
Password: *****  
[arc04]: PS C:\Users\Administrator\Documents>
```

Generally available

# Azure Virtual Network Manager

## The order of network traffic evaluation:

Security admin rules are evaluated prior to NSG rules

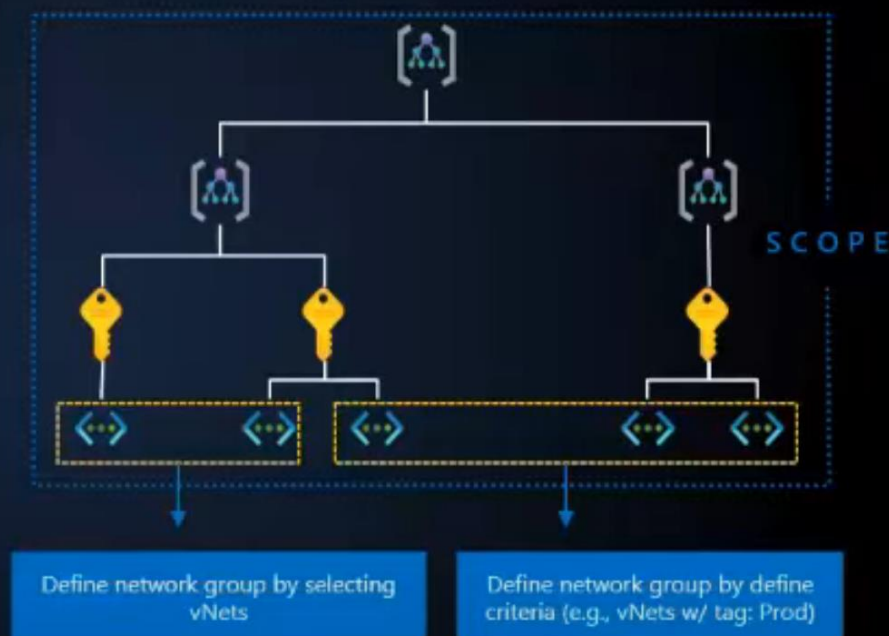


Protect your network resources at scale using security admin rules

# Why we need security admin rules: Security at Scale

## Protect resources in virtual networks at scale

- Day 0 Protection
  - As a network administrator, I want to have all resources protected by default from the moment they're provisioned.
- Emergency Patching at Scale
  - As a security operator, I want to quickly block high-risk traffic and protect all machines at scale once I identify it.

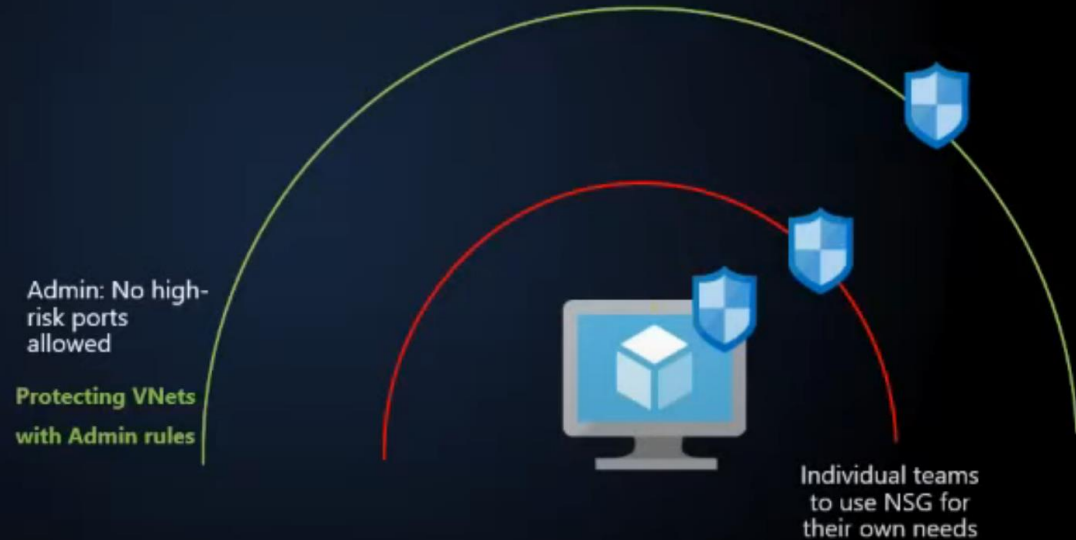


# Security admin rules

Secure at scale with admin rules

## Admin rule (not NSG)

- Target audience: network admins, central governance teams, etc.
- Admin level rules applied to all resources in desired network groups
  - Admin rules to enforce admin's desired network security rules
- Input: security policy --> Output: admin rule
- New VMs will get these rules after they are created
- Enforced rules



# New network security solutions

Cost-effective network security solutions for SMB customers

In preview

**Azure  
Firewall Basic**

In preview

**Azure DDoS  
IP Protection**

# Azure Firewall SKUs

Feature Category	Feature	Firewall Basic <i>Public Preview</i>	Firewall Standard	Firewall Premium
L3-L7 Filtering	Application level FQDN filtering (SNI based) for HTTPS/SQL	✓	✓	✓
	Network level FQDN filtering – all ports and protocols		✓	✓
	Stateful firewall (5 tuple rules)	✓	✓	✓
	Network Address Translation (SNAT+DNAT)	✓	✓	✓
Reliability & Performance	Availability zones	✓	✓	✓
	Built-in HA	✓	✓	✓
	Cloud scalability (auto-scale as traffic grows)	Up to 250Mbps	Up to 30 Gbps	Up to 100 Gbps
	Fat Flow support	N/A	1 Gbps	10 Gbps
Ease of Management	Central management via Firewall Manager	✓	✓	✓
	Policy Analytics (Rule Management over time)	✓	✓	✓
Enterprise Integration	Full logging including SIEM integration	✓	✓	✓
	Service Tags and FQDN Tags for easy policy management	✓	✓	✓
	Easy DevOps integration using REST/PS/CLI/Templates/ Terraform	✓	✓	✓
	Web content filtering (web categories)		✓	✓
	DNS Proxy + Custom DNS		✓	✓
Advanced Threat Protection	Threat intelligence-based filtering (known malicious IP address/ domains)	Alert	✓	✓
	Inbound TLS termination (TLS reverse proxy)			Using App GW
	Outbound TLS termination (TLS forward proxy)			✓
	Fully managed IDPS			✓
	URL filtering (full path - incl. SSL termination)			✓

# Azure DDoS SKUs

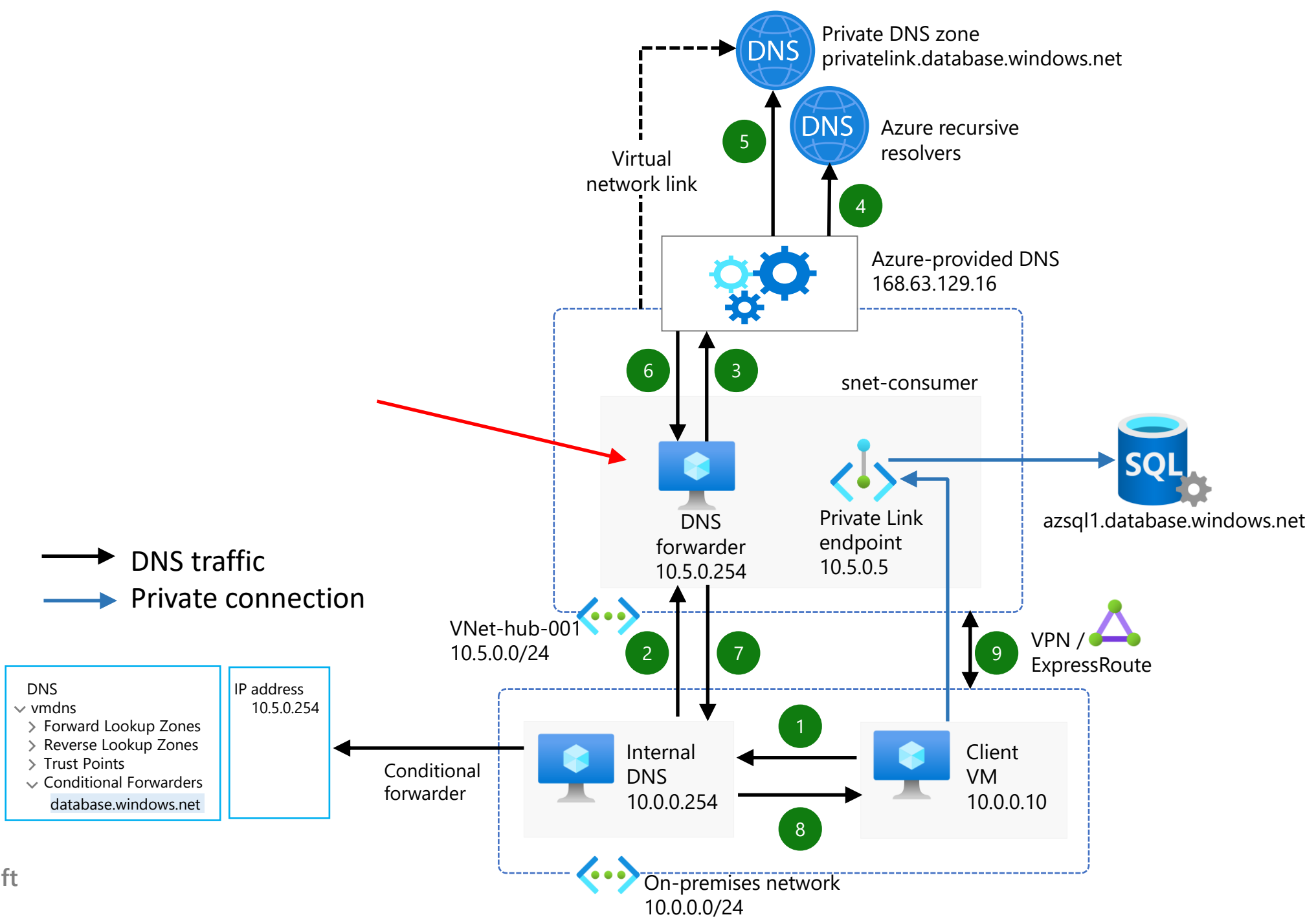
Feature	DDoS IP Protection (Preview)	DDoS Network Protection
Active traffic monitoring & always on detection	✓	✓
L3/L4 Automatic attack mitigation	✓	✓
Automatic attack mitigation	✓	✓
Application based mitigation policies	✓	✓
Metrics & alerts	✓	✓
Mitigation reports	✓	✓
Mitigation flow logs	✓	✓
Mitigation policies tuned to customers application	✓	✓
Integration with Firewall Manager	✓	✓
Azure Sentinel data connector and workbook	✓	✓
DDoS rapid response support		✓
Cost protection		✓
WAF discount		✓

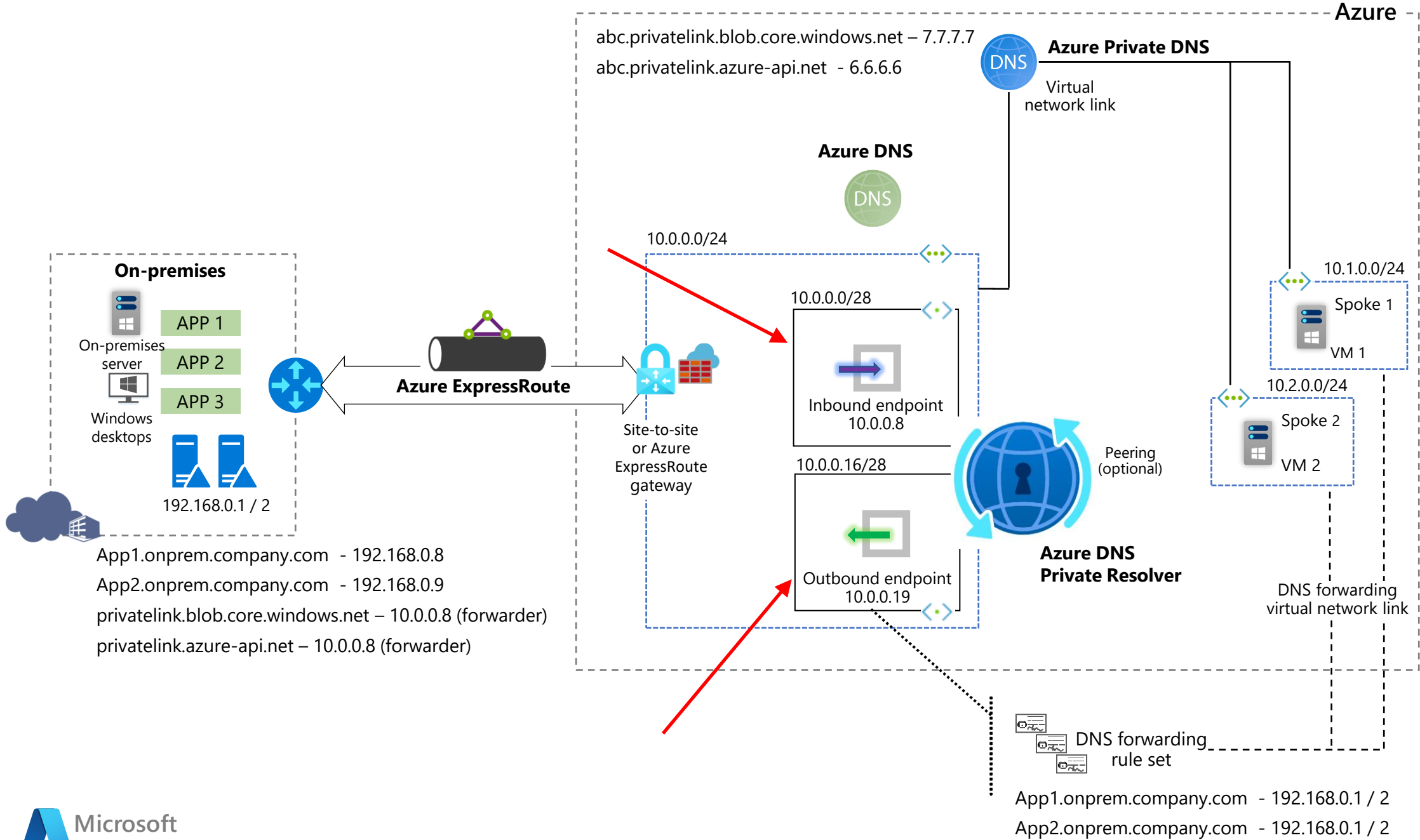
# Azure DNS Private Resolver - GA



- Fully managed DNS resolver
- Inbound endpoints – query private Azure DNS zones from on-premises
- Outbound endpoints – Conditional forwarding from Azure to on-premises
  - Requires dedicated subnet









Generally available

# Azure Disk Storage Premium SSD v2

Data-intensive workloads

Low latency and high performance

Flexible provisioning

Shared block storage

Up to  
**64TiB**  
capacity

Up to  
**80K**  
IOPS

---

**<1ms**  
avg latency

**1200 MB/s**  
throughput

In preview

# Azure Elastic SAN

Cloud native

Fully managed

Massively scalable

- 1-100 TiB
- 500.000 IOPS
- 8.000 MB/s

Cost efficient





Azure Infrastructure as a Service



Azure management



# Azure Monitor

Best-in-class observability  
solution for cloud and hybrid



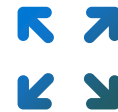
Monitoring is just there and  
works across Azure and hybrid

---



Ability to observe at any  
level and across the stack

---



Open and extensible  
platform for innovation

---



Enterprise ready for  
mission critical scenarios



New Azure Monitor capabilities further modernize your environments for agility and optimize costs

Generally available

## Predictive autoscale

Intelligently scale your Virtual Machine Scale Sets ahead of demand

Generally available

## Basic logs and data archive

Ingest logs at a fifth of current costs and archive data for up to 7 years

Generally available

## Azure Monitor Agent

Migration tool GA – Move from old Log Analytics Agent

Windows 10/11 GA

# Update Management Center

- Central overview of all machines the user has access to through RBAC

