Microsoft

AZ-800 Administer Windows Server Hybrid Core Infrastructure

Agenda AZ-800

1 Deploy and manage identity infrastructure – Windows Server

2 Deploy and manage identity infrastructure – Hybrid

3 Administering Windows Server Hybrid Core Infrastructure – Windows Server

4 Administering Windows Server Hybrid Core Infrastructure – Hybrid

5 Manage virtualization and containers – Windows Server

6 Manage virtualization and containers – Hybrid

7 Implement and manage networking infrastructure – Windows Server

8 Implement and manage networking Infrastructure – Hybrid

9 Configure storage and file services – Windows Server

10 Configure storage and file services – Hybrid

Administer Windows Server Hybrid Core Infrastructure *(Facilitating hybrid management)*

- Administer and manage Windows Server IaaS virtual machines remotely
- Manage hybrid workloads with Azure Arc
- Lab 04 – Using Windows Admin Center in Hybrid Scenarios

Administer and manage Windows Server IaaS virtual machines remotely

Learning Objectives – Remote management of Windows Server IaaS virtual machines

- Choosing the appropriate remote administration tool
- Demonstration - Using Windows Admin Center
- Configure just-in-time administration (JIT)
- Demonstration - Configuring and using JIT access
- Manage Windows VMs with Azure Bastion
- Learning recap

Select the appropriate remote administration tool

Azure portal ✓

Windows Admin Center ✓

Azure PowerShell

Azure CLI

Run Command

Azure Cloud Shell ✓

Install-Module Az

Az.Network
Az.Compute
Az. ...

Demonstration – Use Windows Admin Center to manage a Windows Server VM

Ensure the Azure VM meets the requirements

Install Windows Admin Center in the VM you plan to manage

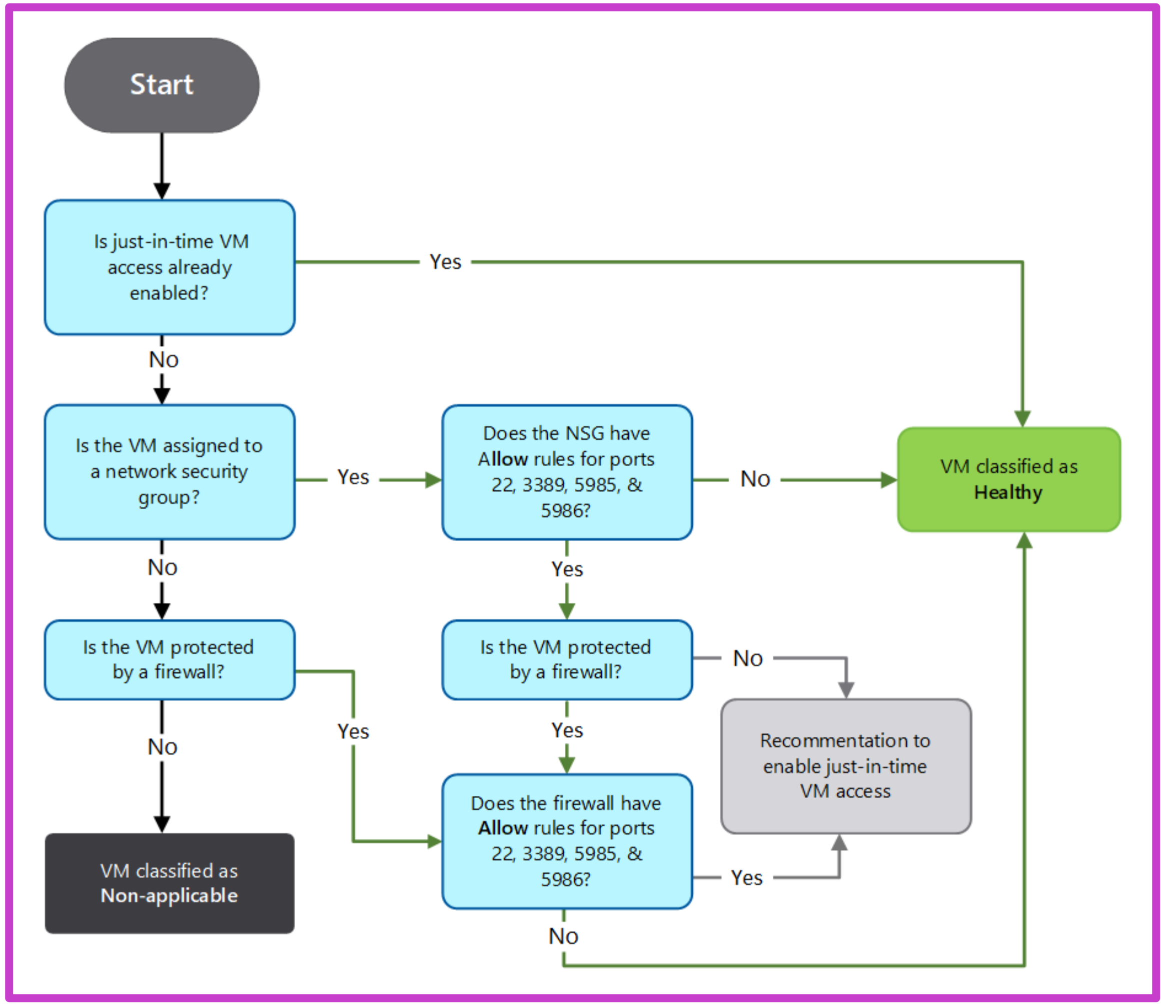
Connect to Windows Admin Center and use it to manage the VM

Specify port rules for inbound connections

Configure Just-in-time Administration (1/2)

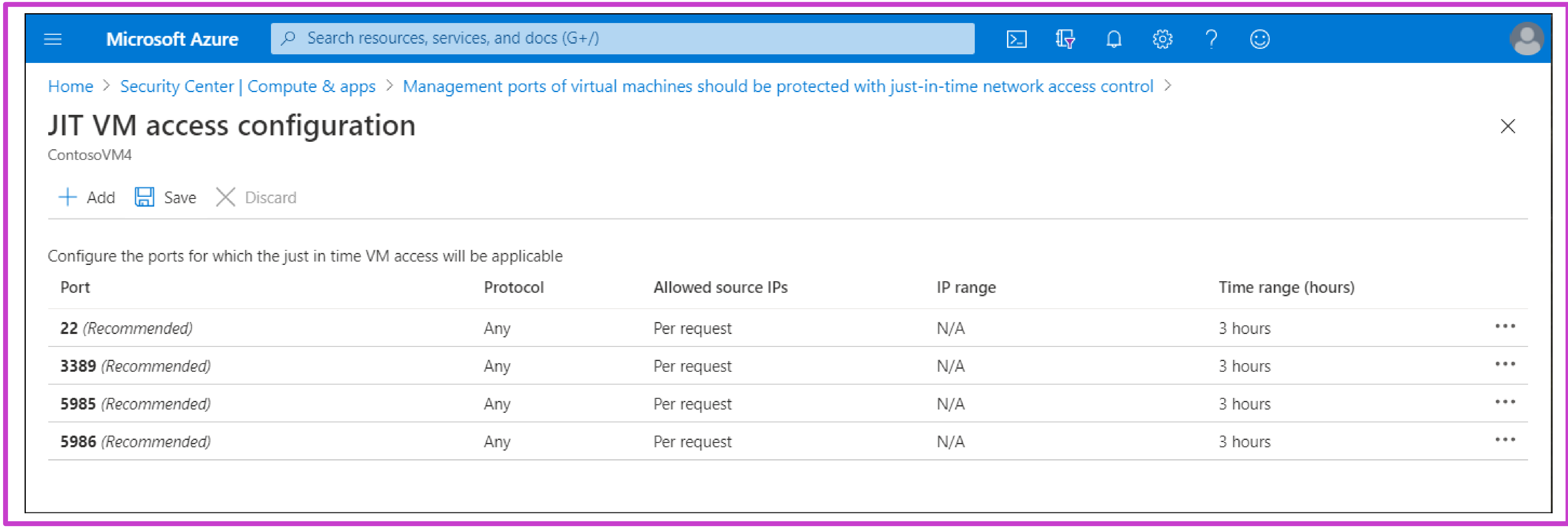
How does JIT administration work?

- You enable JIT for VMs through the Microsoft Defender for Cloud
- You can then define the network ports
- Microsoft Defender for Cloud imposes a deny all inbound traffic rule for your selected ports by using the NSG and Azure Firewall rules.
- JIT is a paid feature of Microsoft Defender for Cloud



Start
Is just-in-time VM access already enabled?
Yes
No
Is the VM assigned to a network security group?
Yes
No
Does the NSG have **Allow** rules for ports 22, 3389, 5985, & 5986?
No
Yes
VM classified as **Healthy**
Is the VM protected by a firewall?
Yes
No
Is the VM protected by a firewall?
No
Yes
Recommentation to enable just-in-time VM access
Does the firewall have **Allow** rules for ports 22, 3389, 5985, & 5986?
Yes
No
VM classified as **Non-applicable**

Configure Just-in-time Administration (2 of 2)


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Security Center | Compute & apps > Management ports of virtual machines should be protected with just-in-time network access control >

JIT VM access configuration

ContosoVM4

Configure the ports for which the just in time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)
22 *(Recommended)*	Any	Per request	N/A	3 hours
3389 *(Recommended)*	Any	Per request	N/A	3 hours
5985 *(Recommended)*	Any	Per request	N/A	3 hours
5986 *(Recommended)*	Any	Per request	N/A	3 hours

Demonstration – Configuring and using JIT Access to allow remote management to a Windows Server VM in Azure

Enable JIT on VMs from Microsoft Defender for Cloud

Edit the JIT configuration on a JIT-enabled VM using Defender for Cloud

Request access to a JIT-enabled VM

Audit JIT access activity in Defender for Cloud

Manage Windows virtual machines with Azure Bastion (1/3)

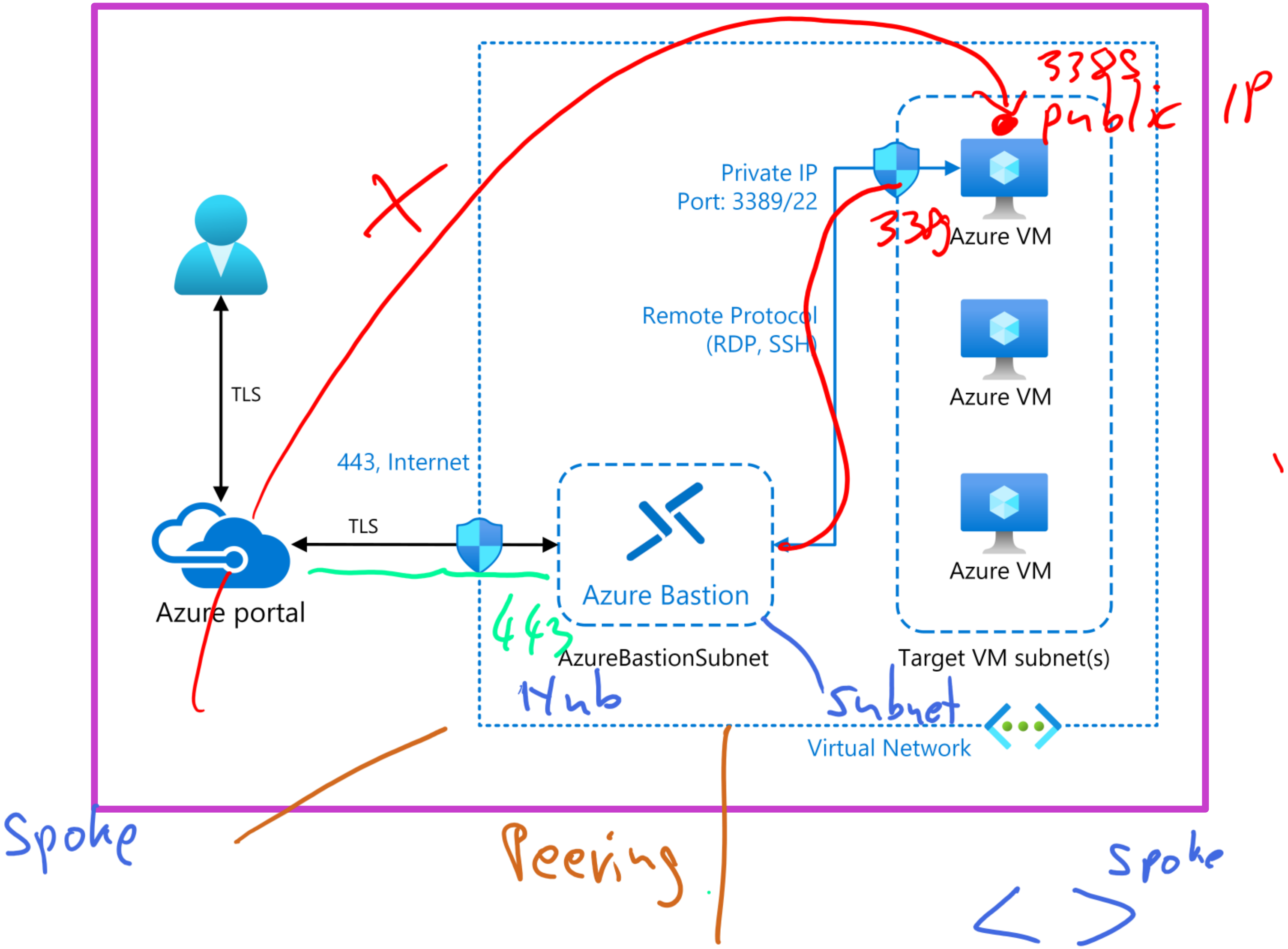
Azure Bastion provides secure RDP and SSH connectivity to all the VMs in the same VNet or peered VNets

Bastion host servers:

- Are designed and configured to withstand attacks.
- Provide RDP and SSH connectivity to your Azure workloads behind the bastion.

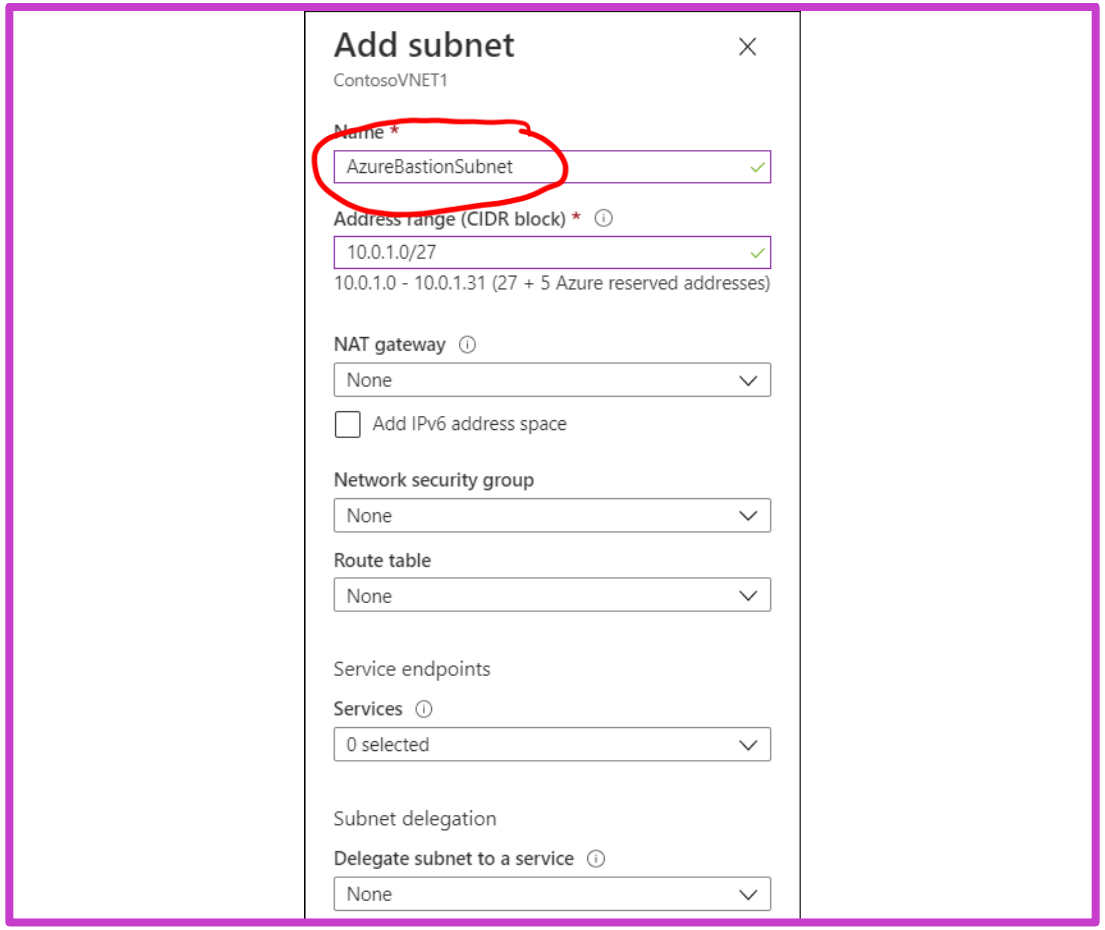
Only the Bastion requires a public IP, not the VMs it's protecting

SKU Developer or
Basic
Standard



Manage Windows virtual machines with Azure Bastion (2/3)

Deploy a bastion host



Add subnet

ContosoVNET1

Name *

AzureBastionSubnet

Address range (CIDR block) *

10.0.1.0/27

10.0.1.0 - 10.0.1.31 (27 + 5 Azure reserved addresses)

NAT gateway: None

□ Add IPv6 address space

Network security group: None

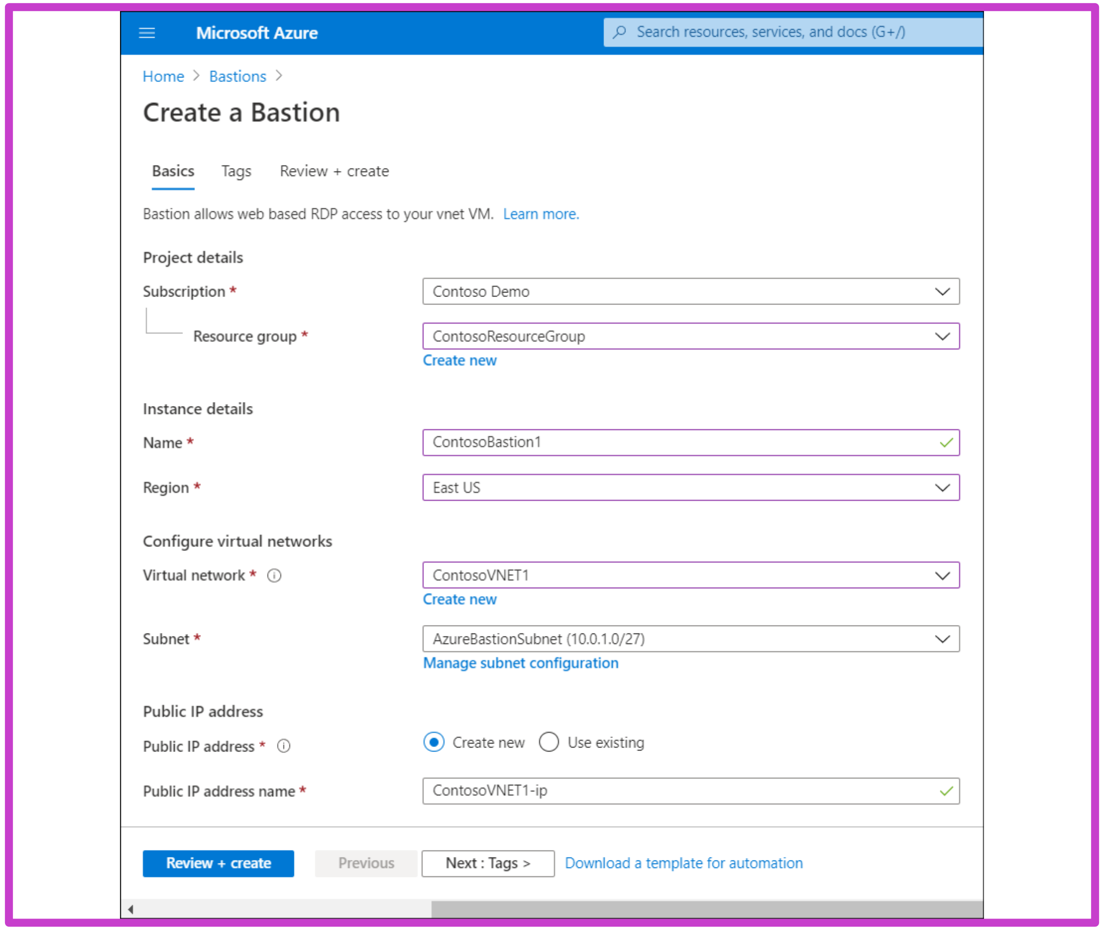
Route table: None

Service endpoints

Services: 0 selected

Subnet delegation

Delegate subnet to a service: None



Home > Bastions >

Create a Bastion

Bastion allows web based RDP access to your vnet VM. Learn more.

Project details

Subscription *: Contoso Demo

Resource group *: ContosoResourceGroup

Create new

Instance details

Name *: ContosoBastion1

Region *: East US

Configure virtual networks

Virtual network *: ContosoVNET1

Create new

Subnet *: AzureBastionSubnet (10.0.1.0/27)

Manage subnet configuration

Public IP address

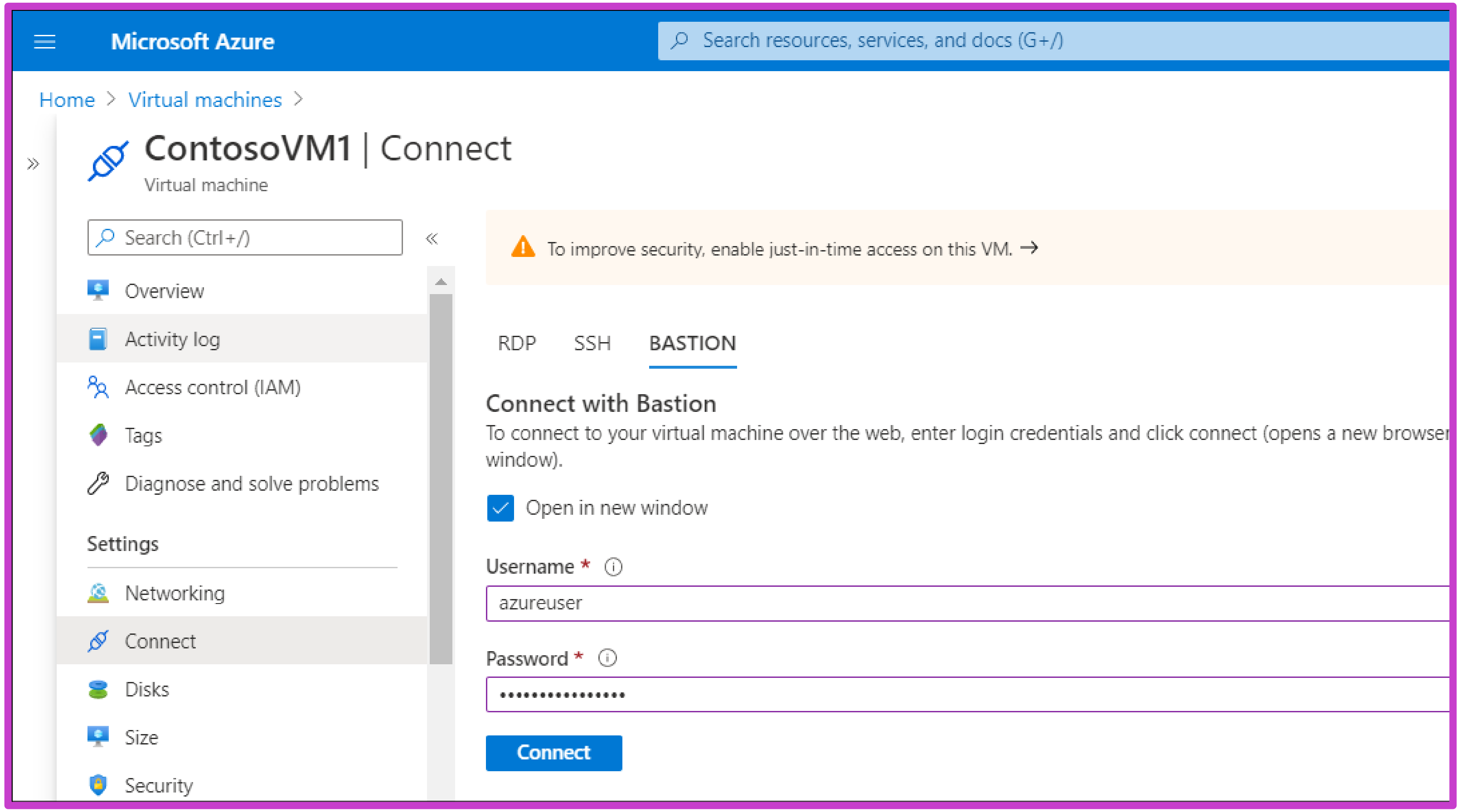
Public IP address *: ● Create new ○ Use existing

Public IP address name *: ContosoVNET1-ip

Manage Windows virtual machines with Azure Bastion (3/3)

Use the following procedure to connect to a Windows VM using Azure Bastion:

1. Navigate to the VM to which you want to connect.
2. Select the VM, and on the Virtual machine blade, select Connect.
3. In the Connect drop-down list, select Bastion.
4. Enter the credentials of a user with appropriate permissions, and then select Connect.



ContosoVM1 | Connect

Virtual machine

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

Connect with Bastion

To connect to your virtual machine over the web, enter login credentials and click connect (opens a new browser window).

☑ Open in new window

Username * : azureuser

Password * : ••••••••••••••••

Demonstration – Create an Azure Bastion host

Extend the virtual network associated with Contoso VM1

Create the AzureBastionSubnet

Configure a Bastion instance

Connect to VM1 using the Bastion connection

Learning recap – Remote management Of Windows Server IaaS VMs

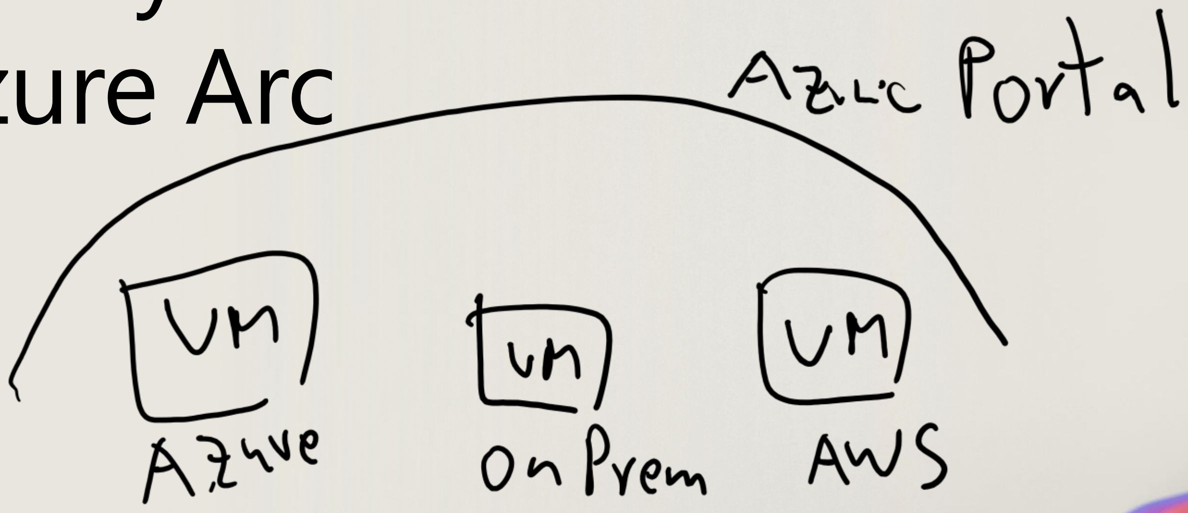
Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Administer and manage Windows Server IaaS Virtual Machine remotely

Manage hybrid workloads with Azure Arc

VM
SQL MI
K8S



Learning Objectives – Manage hybrid workloads with Azure Arc

- Describe Azure Arc
- Onboard Windows Server instances
- Demonstration – Connect hybrid servers to Azure Arc
- Use Azure Arc to manage Windows Server instances
- Restrict access with RBAC
- Learning recap

Describe Azure Arc

Azure Arc is a service that provides a set of technologies for organizations

It provides a centralized, unified, and self-service approach to managing:

- Windows Server ✓
- Linux servers ✓
- Kubernetes clusters ✓
- Azure Data Services ✓

ARC Agent

Azure Arc capabilities

- Features available to registered systems
  - Azure Machine Configuration
  - Support for resource-context–access Log Analytics data
  - Microsoft Defender for Cloud ✓
  - Microsoft Sentinel SIEM
  - Azure Monitor
  - Azure Update Manager

Onboard Windows Server instances

Deploy Azure Arc to on-premises computers and hybrid cloud computers

1. Must have the correct permissions as administrator
    - Member of the Azure Connected Machine Onboarding role
    - Member of the Azure Connected Resource Administrator role
2. Install the Azure Connected Machine agent on each of the operating systems targeted for Azure Resource Manager-based management
3. Manage the onboarding of Windows Server instances from Azure Arc.

Demonstration – Connect hybrid servers to Azure Arc

Generate the installation script from the Azure portal

Install and validate the Azure Connected Machine Agent on Windows

Verify the connection with Azure Arc

On-premises server is now listed as an Azure Arc machine

Use Azure Arc to manage Windows Server instances (1/3)

Extension	Additional information
CustomScriptExtension ✓	Downloads and executes scripts on Azure VMs
Azure Key Vault ?	Provides automatic refresh of certificates stored in an Azure key vault
Azure Monitor Agent ✓	Collects monitoring data from the guest operating system of Azure and hybrid virtual machines
Azure Extension for SQL Server	Initiates a SQL Server connection to Azure

Manage extensions

- VM extensions are small apps that provide post-deployment configuration and automation tasks on Azure VMs.
- Azure Arc for servers enables you to deploy Azure VM extensions to both non-Azure Windows and Linux VMs; this can help to simplify management of those computers.
- You can add the extensions listed and described in the table, to an Azure Arc VM.

Use Azure Arc to manage Windows Server instances (2/3)

Manage Azure Policy

- Azure Policy – service that can help organizations manage and evaluate compliance.
- Uses declarative rules based on properties of target Azure resource types.
- Azure Arc lets you to extend some capabilities of Azure Policy to operating systems of computers running in on-premises datacenters or hosted by third-party cloud providers.

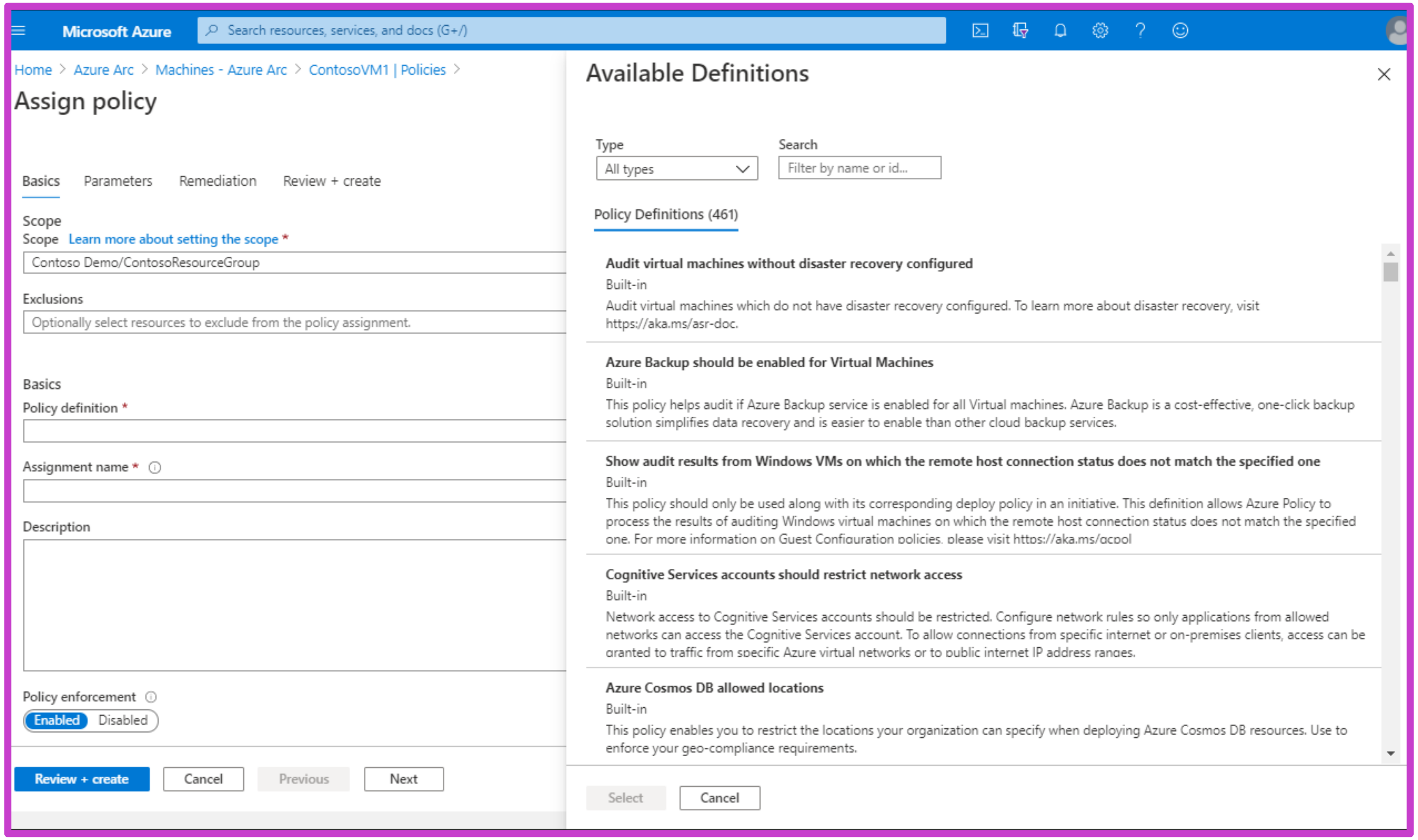
Azure Policy functionality can be grouped into four main categories:

- Enforcing compliance when provisioning new Azure resources
- Auditing compliance of existing Azure resources
- Remediating non-compliance of existing Azure resources
- Auditing compliance of the OS, application configuration, and environment settings within Azure VMs

Use Azure Arc to manage Windows Server instances (3/3)

Assign Azure Arc policies

- In Azure portal, navigate to Azure Arc, and then **Manage servers**
- Select the appropriate server, and then select **Policies**.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Arc > Machines - Azure Arc > ContosoVM1 | Policies >
Basics
Parameters
Remediation
Review + create
Review + create
Cancel
Previous
Next
Select
Cancel

Assign policy

Scope

Scope Learn more about setting the scope *

Contoso Demo/ContosoResourceGroup

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition *

Assignment name *

Description

Policy enforcement

Enabled Disabled

Available Definitions

Type: All types

Search: Filter by name or id...

Policy Definitions (461)

Audit virtual machines without disaster recovery configured

Built-in

Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit https://aka.ms/asr-doc.

Azure Backup should be enabled for Virtual Machines

Built-in

This policy helps audit if Azure Backup service is enabled for all Virtual machines. Azure Backup is a cost-effective, one-click backup solution simplifies data recovery and is easier to enable than other cloud backup services.

Show audit results from Windows VMs on which the remote host connection status does not match the specified one

Built-in

This policy should only be used along with its corresponding deploy policy in an initiative. This definition allows Azure Policy to process the results of auditing Windows virtual machines on which the remote host connection status does not match the specified one. For more information on Guest Configuration policies, please visit https://aka.ms/gcpol

Cognitive Services accounts should restrict network access

Built-in

Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.

Azure Cosmos DB allowed locations

Built-in

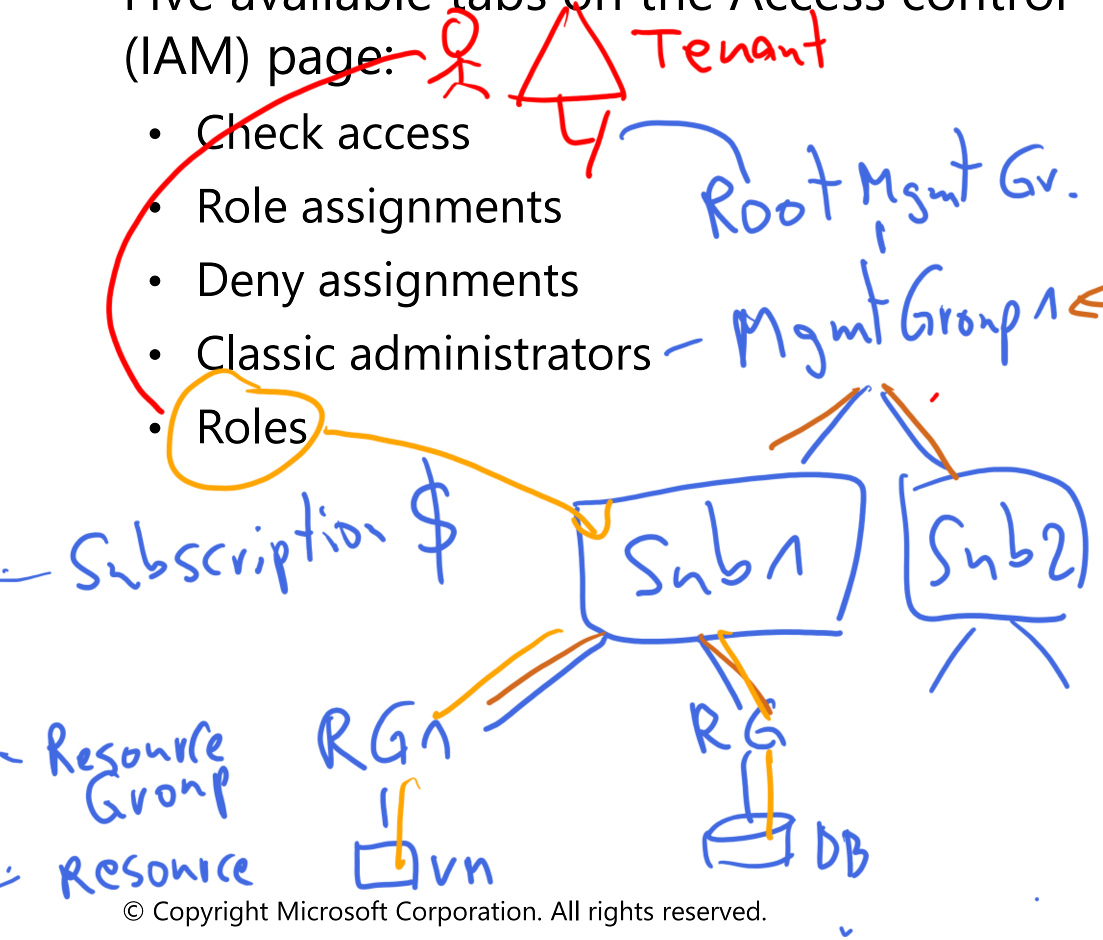
This policy enables you to restrict the locations your organization can specify when deploying Azure Cosmos DB resources. Use to enforce your geo-compliance requirements.

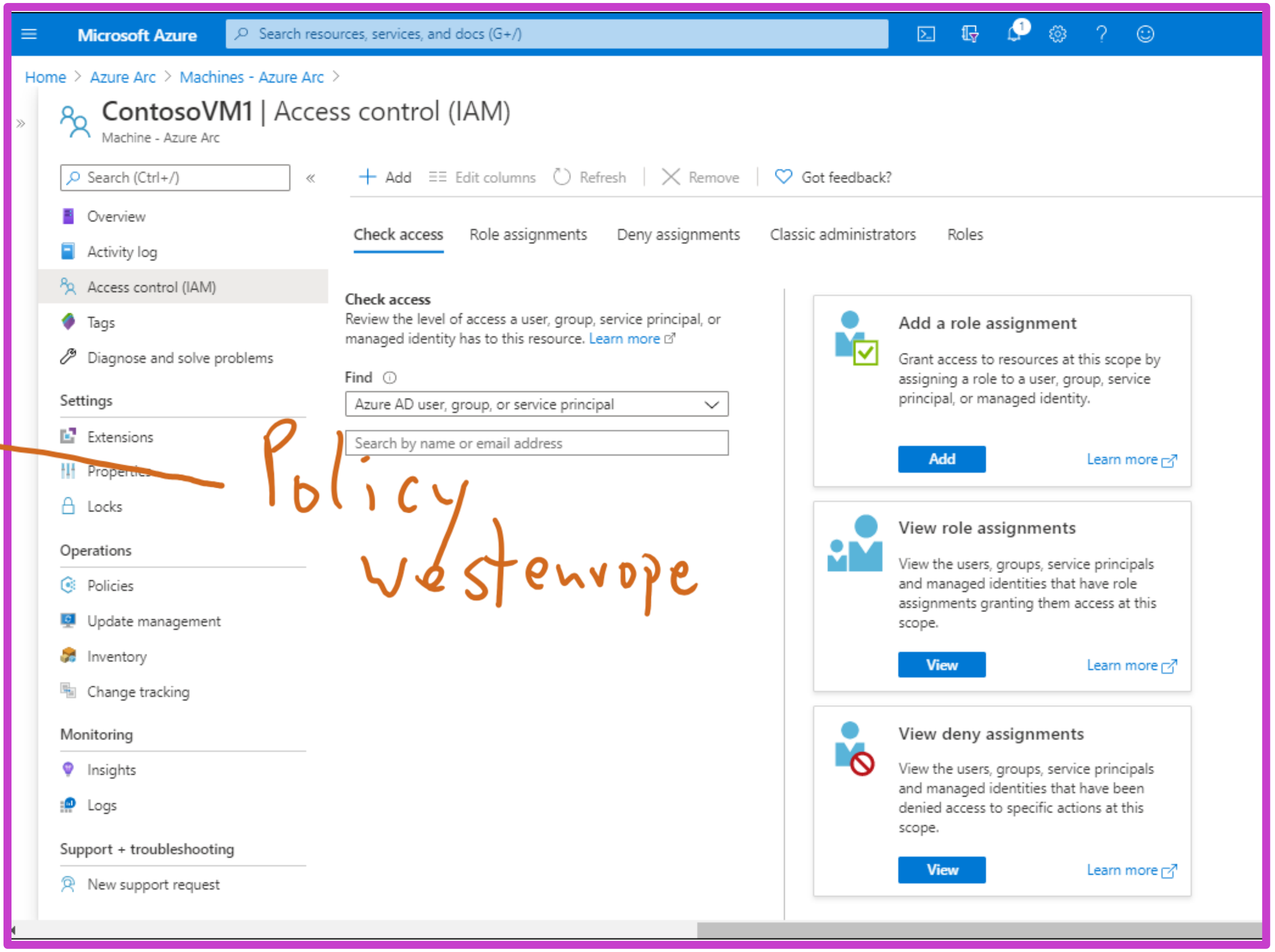
Restrict access to VMs with RBAC

Manage access

Five available tabs on the Access control (IAM) page:

- Check access
- Role assignments
- Deny assignments
- Classic administrators
- Roles





Home > Azure Arc > Machines - Azure Arc >

ContosoVM1 | Access control (IAM)

Machine - Azure Arc

Search (Ctrl+/) «

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

Settings
Extensions
Properties
Locks

Operations
Policies
Update management
Inventory
Change tracking

Monitoring
Insights
Logs

Support + troubleshooting
New support request

+ Add | Edit columns | Refresh | Remove | Got feedback?

Check access | Role assignments | Deny assignments | Classic administrators | Roles

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: Azure AD user, group, or service principal

Search by name or email address

Add a role assignment

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

Add | Learn more

View role assignments

View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

View | Learn more

View deny assignments

View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

View | Learn more

Learning recap – Manage hybrid workloads with Azure Arc

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Manage hybrid workloads with Azure Arc

Lab 04 – Using Windows Admin Center in hybrid scenarios

Lab 04: Using Windows Admin Center in hybrid scenarios

Lab scenario

To address concerns regarding the consistent operational and management model, regardless of the location of managed systems, you'll test the capabilities of Windows Admin Center in the hybrid environment containing different versions of the Windows Server operating system running on-premises and in Microsoft Azure virtual machines (VMs).

Objectives

- Test hybrid connectivity by using Azure Network Adapter.
- Deploy Windows Admin Center gateway in Azure.
- Verify functionality of Windows Admin Center gateway in Azure.

End of Presentation