



Lab 2 8921

By Trevor Kutto

Allowed locations ...

Policy definition

[Assign policy](#) [Edit definition](#) [Duplicate definition](#) [Select version](#) [Delete definition](#)

Essentials

Name	: Allowed locations	Definition location	: --
Version	: 1.0.0	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-...
Description	: This policy enables you to restrict the locations your organization can specify whe...	Type	: Built-in
Available Effects	: Deny	Mode	: Indexed
Category	: General		

Definition Assignments (0) Parameters (1)

```
1 {
2   "properties": {
3     "displayName": "Allowed locations",
4     "policyType": "BuiltIn",
5     "mode": "Indexed",
6     "description": "This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requireme",
7     "metadata": {
8       "version": "1.0.0",
9       "category": "General"
10    },
11    "version": "1.0.0",
```

Creation of the allowed location policy above is shown

Create a virtual machine ...

i This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

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

Subscription *	<input type="text" value="Azure for Students"/>
Resource group *	<input type="text" value="policy"/> Create new

Instance details

Virtual machine name *	<input type="text" value="policytest"/>
Region *	<input type="text" value="(US) East US"/> Deploy to an Azure Extended Zone

x This policy maintains a set of best available regions where your subscription can deploy resources. The objective of this policy is to ensure that your subscription has full access to Azure services with optimal performance. Should you need additional or different regions, contact support.

Availability options	<input type="text" value="Availability zone"/>
----------------------	--

[< Previous](#)

[Next : Disks >](#)

[Review + create](#)

The policy is enforced for this instance and no resource can be created here unless it is canada central and it gives us a warning if we try continue and do this thus showing enforcement of the policy

Create virtual network ...



✓ Validation passed

Basics Security IP addresses Tags Review + create

[View automation template](#)


Basics




Subscription	Azure for Students
Resource Group	policy
Name	policyVN
Region	Canada Central

Security


Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled





IP addresses


 **policyVN**
Virtual network


  ... 


Diagnose issues with this virtual network +2





 Move  Delete  Refresh  Give feedback


 **Overview**

 Activity log

 Access control (IAM)

 Tags

 Diagnose and solve problems


 Resource visualizer

> Settings

> Monitoring

> Automation

> Help

 **Essentials** [JSON View](#)

Resource group (... : [policy](#)

Location ([move](#)) : Canada Central

Subscription (... : [Azure for Students](#)

Subscription ID : acc96d9d-e040-48a5-9191-cd80276cb66d

Address space : [10.0.0.0/16](#)

Subnets : [1 subnet](#)

DNS servers : [Azure provided DNS service](#)

BGP community s... : [Configure](#)

Virtual network ID : 26477f30-4cc6-4341-a241-9dce23cbe884

Tags ([edit](#)) : [Add tags](#)

Topology Properties Capabilities (5) Recommendations

Tutorials

The virtual network is created and follows the policy we enforced in canada central

policyVN | Subnets Virtual network Analyze connectivity issues in this virtual network +2

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
 - Address space
 - Connected devices
 - Subnets**
 - Bastion
 - DDoS protection
 - Firewall

+ Subnet **Refresh** | **Manage users** **Delete** **...**

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

Search subnets

<input type="checkbox"/>	Name ↑	IPv4	IPv6	Available IPs
<input type="checkbox"/>	default	10.0.0.0/24	-	251
<input type="checkbox"/>	Private-subnet	10.0.1.0/24	-	251
<input type="checkbox"/>	Public-subnet	10.0.2.0/24	-	251

Public subnets and private subnets created as shown above on the virtual network made

Home > Private-subnet-nsg

Private-subnet-nsg | Outbound security rules Network security group

Search

+ Add **Hide default rules** **Refresh** **Delete** **Give feedback**

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	Allow_azure-storage	8080	Any	Any	Storage	Allow
200	Deny-internet-access	8080	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Outbound security rules after creation of the private subnet nsg

Network foundation | Network security... Preview

Search

+ Create **Manage view** **...**

Overview

- Virtual network overview
 - Virtual networks
 - NAT gateways
 - Public IP addresses
- Network interfaces
- Network security groups**
 - Application security groups
 - Bastions
 - Route tables
 - Route servers
- Private Link
- DNS

Private-subnet-nsg | Inbound security rules Network security group

Search

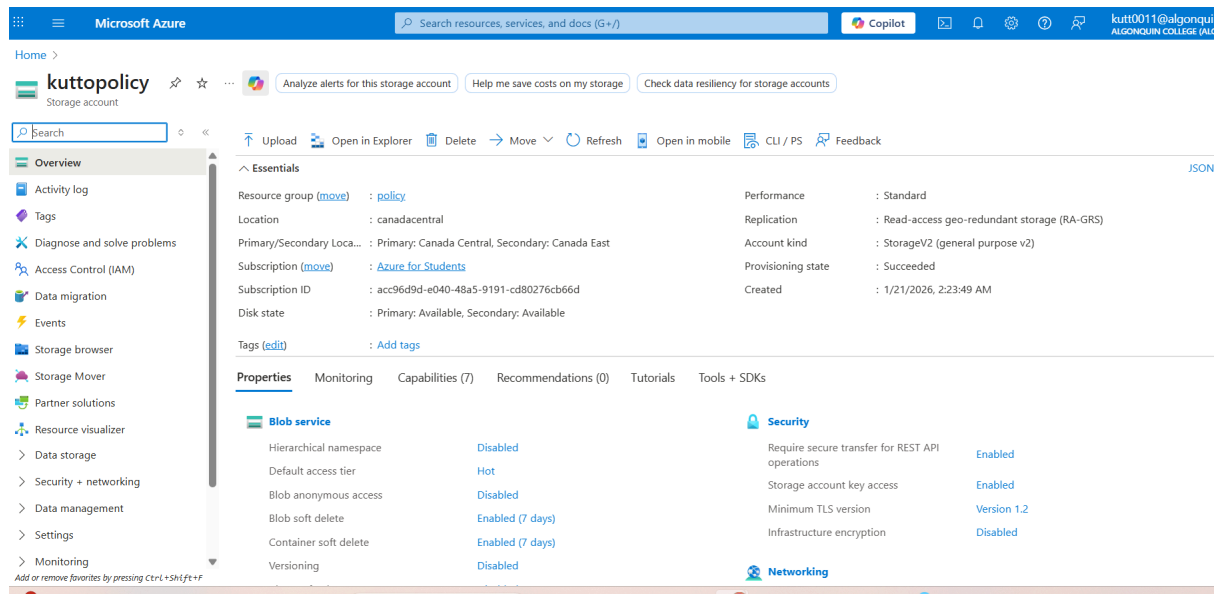
+ Add **Hide default rules** **Refresh** **Delete** **Give feedback**

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source
210	Allow-rdp	3389	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalanc...	Any	Any	Azure
65500	DenyAllInBound	Any	Any	Any

Allowing of RDP in the inbound rules is created above



Storage account created successfully

Create a virtual machine

✓ Validation passed

Subscription	Azure for Students
Resource group	policy
Virtual machine name	Vm-private
Region	Canada Central
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2022 Datacenter: Azure Edition - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	kutt0011
Already have a Windows license?	No
Azure Spot	No

Vm-private - windows overview files

✓ Validation passed

Subscription	Azure for Students
Resource group	policy
Virtual machine name	Vm-public
Region	Canada Central
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2022 Datacenter: Azure Edition - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	kutt0011
Public inbound ports	RDP

Vm-public overview page windows

Basics Advanced Tags Review + create

Summary

Basics

Name	kutt0011bastion
Subscription	Azure for Students
Resource group	policy
Region	Canada Central
Availability zone	1, 2, 3
Virtual network	policyVN (policy)
Tier	Standard
Subnets	AzureBastionSubnet
Public IPv4 address	policyVN-IPv4
Instance count	2
Copy and paste	Enabled
IP-based connection	Disabled
Kerberos authentication	Disabled
Shareable Link	Disabled
Session recording	Disabled
Native client support	Disabled
Private Bastion	Disabled

```
Select Administrator: Windows PowerShell

on
+ FullyQualifiedErrorId : CouldNotMapNetworkDrive,Microsoft.PowerShell.Commands.NewPSDr
iveCommand

PS C:\Users\kutt0011> $key = @{
> String = "<z1T/ZifIrrDIJ9knksROHpWqYn8pGPfBa02c8wotOVR9ELAHSQWvyvt+c+4+h9vLZ7fPjsbSeC
OR+ASTvmAZQA==>"
> }
> $acctKey = ConvertTo-SecureString @key -AsPlainText -Force
> $cred = @{
> ArgumentList = "Azure\<kuttopolicy>", $acctKey
> }
> $credential = New-Object System.Management.Automation.PSCredential @cred
> $map = @{
> Name = "Z"
> PSPProvider = "FileSystem"
> Root = "\\<kuttopolicy>.file.core.windows.net\kuttopolicy"
> Credential = $credential
> }
```

Denied request

poli

Resource

Search

Overview

Activity lo

Access co

Tags

Resource

Events

Settings

Cost Man

Monitorin

Automatic

Help

Delete a resource group

The following resource group and all its dependent resources will be permanently deleted.

Resource group to be deleted

policy

14 resources being deleted across 1 subscriptions, 2 resource groups
All dependent resources, including hidden types, are shown

Name	Resource type	Subscription	Resource Group
kuttolicy	Storage account	Azure for Students	policy
policyVN	Virtual network	Azure for Students	policy
policyVN-bastion	Bastion	Azure for Students	policy
policyVN-IPv4	Public IP address	Azure for Students	policy
Private-subnet-nsg	Network security group	Azure for Students	policy

☒ Apply force delete for selected Virtual machines and Virtual machine scale sets ⓘ

Enter resource group name to confirm deletion *

Delete

Cancel

Cleanup of files and policy plus all other resources