

# Azure Cloud Infrastructure Project (GUI + ARM Template Deployment)

An organisation needs a cloud-based infrastructure on Microsoft Azure to support high availability, secure communication, and resilient storage. This deployment uses the **Azure Portal (GUI)** with an **ARM template** to provision and verify all resources step-by-step.

**Project Github :** <https://github.com/sagarpatalbox/upgrad-azure-project>

**Project Drive :**

<https://drive.google.com/drive/folders/1gQr4-znjALOK8J5izXt4GY0J68CTxOSK>

---

## Task I — Setup Virtual Networks

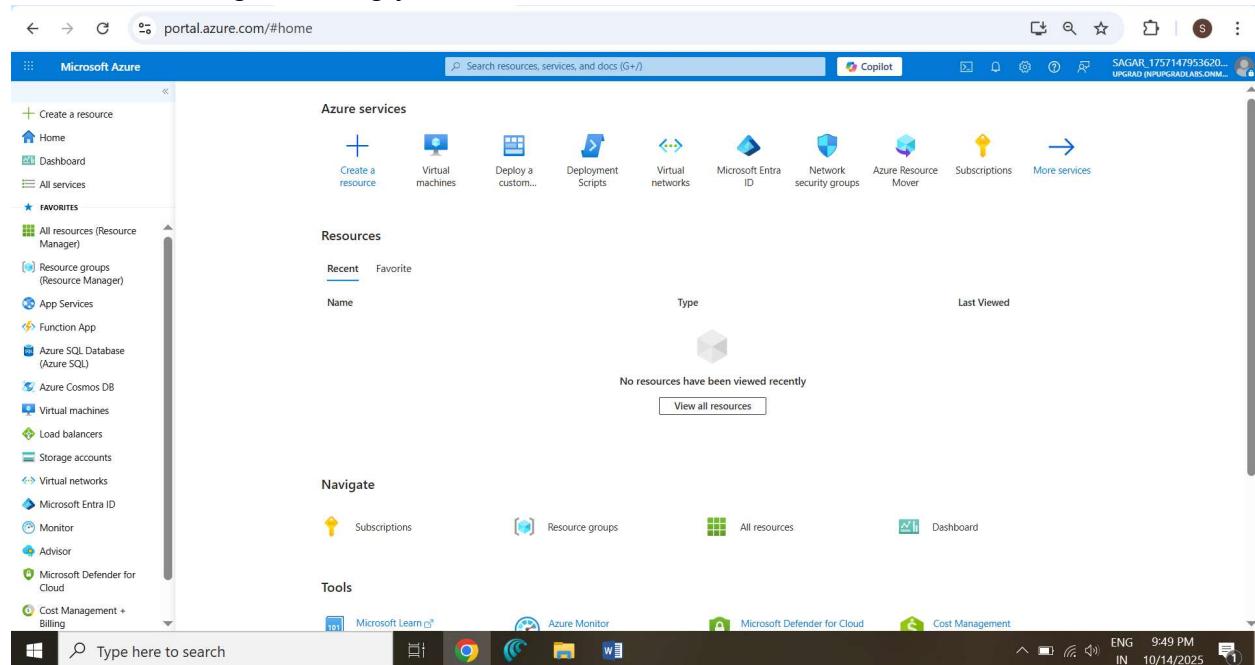
### Objective

Create two virtual networks for resource isolation and establish secure communication between them.

#### ▪ Steps (in Azure Portal GUI)

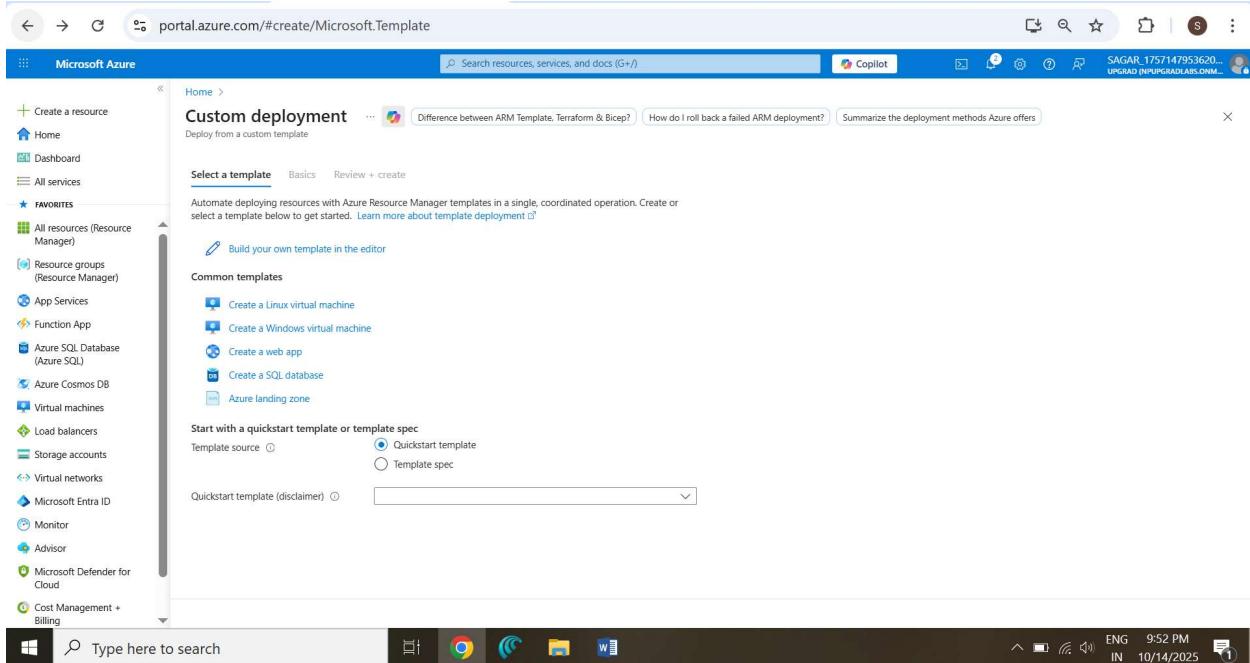
##### 1. Login to Azure Portal

- Go to <https://portal.azure.com>.
- Sign in using your Azure credentials.



## 2. Start Custom Deployment

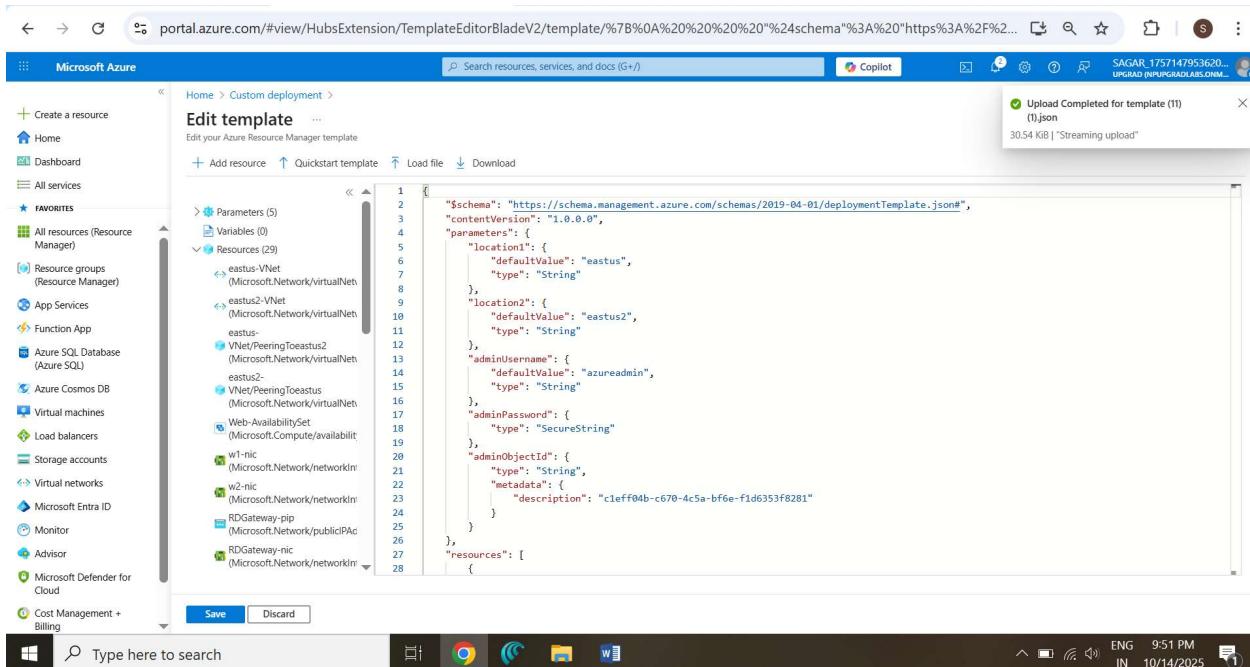
- Search → “Deploy a custom template” → click **Build your own template in the editor**.



The screenshot shows the Microsoft Azure portal's 'Custom deployment' blade. On the left, there's a sidebar with various service links. The main area has a heading 'Custom deployment' with a sub-section 'Select a template'. It offers two main paths: 'Build your own template in the editor' (which is currently selected) and 'Common templates' (which includes options like 'Create a Linux virtual machine', 'Create a Windows virtual machine', 'Create a web app', 'Create a SQL database', and 'Azure landing zone'). Below these, there's a section for 'Start with a quickstart template or template spec'. It includes fields for 'Template source' (set to 'Quickstart template') and 'Quickstart template (disclaimer)'.

## 3. Upload ARM Template File

- Click **Load file** → select `Azure_Project_ARM.json`
- Click **Save**.

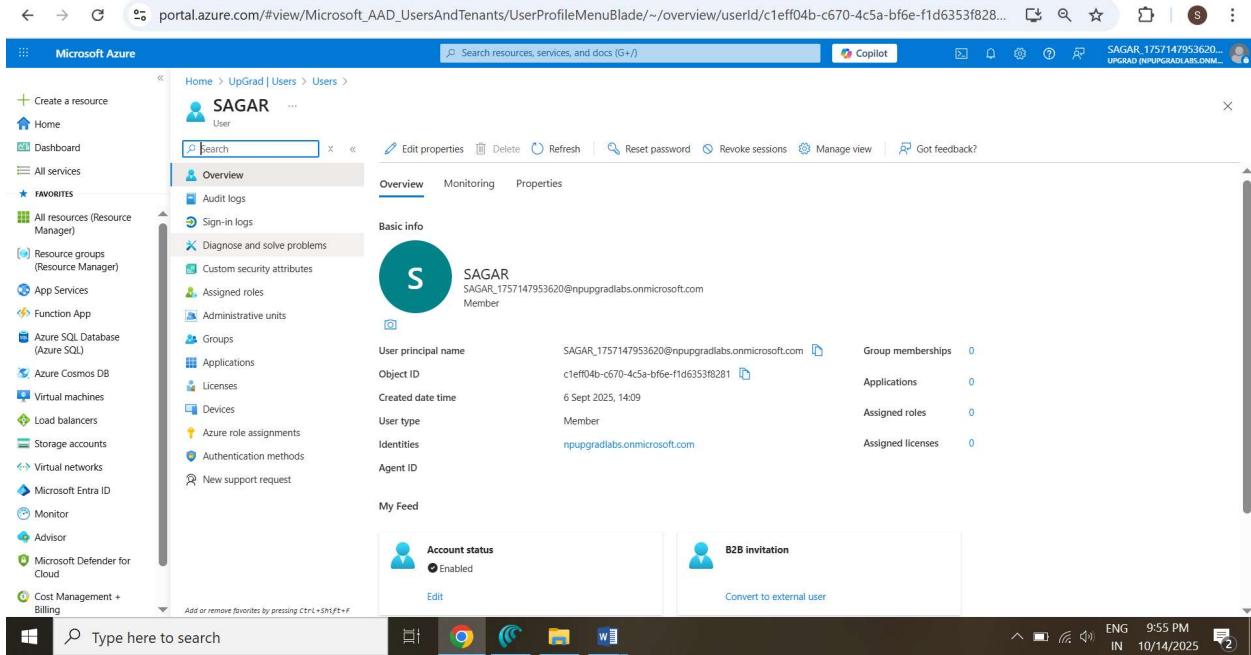


The screenshot shows the Microsoft Azure portal's 'Edit template' blade. The left sidebar is identical to the previous screenshot. The main area shows the ARM template code in a code editor. The code defines a template with parameters, variables, and resources. A success message at the top right says 'Upload Completed for template (1).json'. At the bottom, there are 'Save' and 'Discard' buttons.

```
$schema: "https://schemas.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
contentVersion: "1.0.0.0",
parameters: {
  location1: {
    "defaultValue": "eastus",
    "type": "String"
  },
  location2: {
    "defaultValue": "eastus2",
    "type": "String"
  },
  adminUsername: {
    "defaultValue": "azureadmin",
    "type": "String"
  },
  adminPassword: {
    "type": "SecureString"
  },
  adminObjectId: {
    "type": "String",
    "metadata": {
      "description": "c1eff04b-c670-4c5a-bf6e-f1d6353f8201"
    }
  }
},
resources: [
  {
    ...
  }
]
```

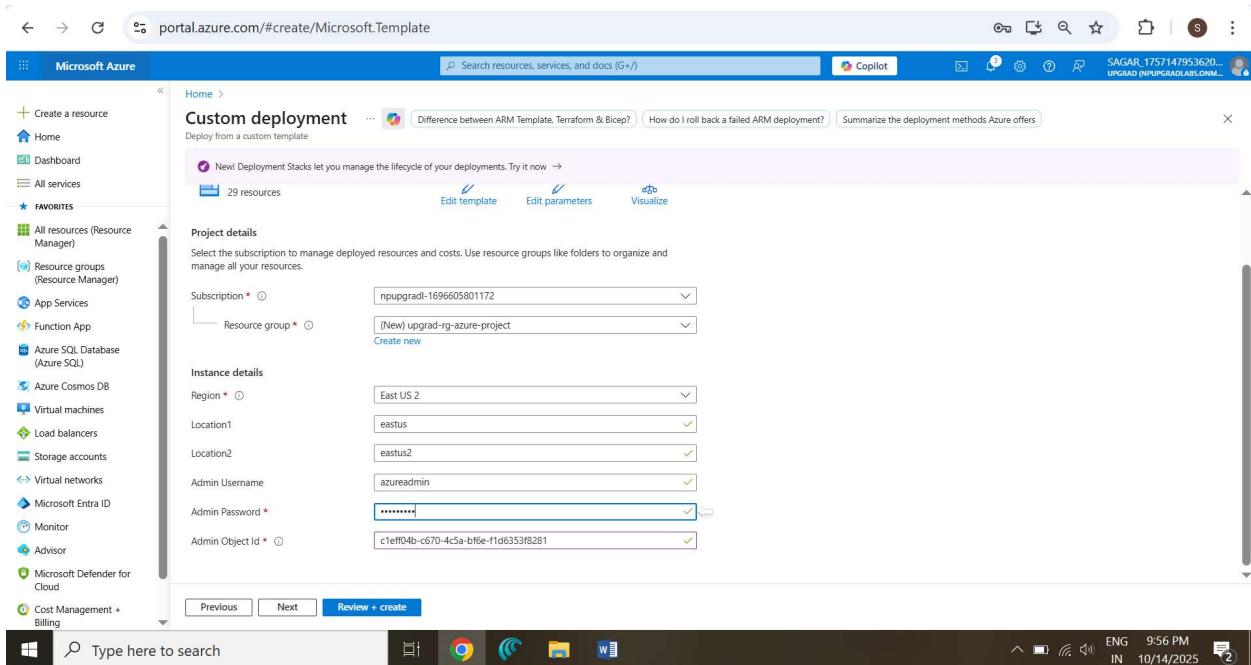
## 4. Configure Deployment Parameters

- **Subscription** → choose active subscription.
- **Resource Group** → “Create new” → `upgrad-rg-azure-project`.
- **Region** → **West US**.
- **Fill parameters** (`adminUsername`, `adminPassword`, `adminObjectId`).
- **Copy Object ID From Below :**



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Home, Dashboard, All services, and Favorites. The main area shows a user profile for 'SAGAR'. Under the 'Overview' tab, the 'Basic info' section displays the user's name, SAGAR, and their object ID, which is highlighted in the screenshot. Other details shown include User principal name, Created date time (6 Sept 2025, 14:09), User type (Member), and Group memberships.

- **Click Review + Create → Create.**



The screenshot shows the 'Custom deployment' step of a deployment template creation wizard. It's a form-based interface with sections for 'Project details' and 'Instance details'. In the 'Project details' section, the 'Subscription' dropdown is set to 'npupgradl-1696605801172' and the 'Resource group' dropdown is set to '(New) upgrad-rg-azure-project'. In the 'Instance details' section, the 'Region' is set to 'East US 2', and the 'Admin Object Id' field contains the value 'c1eff04b-c670-4c5a-bf6e-f1d6353f8281', which matches the one copied from the previous screenshot. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons.

## 5. Monitor Deployment Progress

- Portal → Notifications → view progress.

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation links for creating resources, Home, Dashboard, All services, Favorites, and various Azure services like Resource Manager, App Services, Function App, etc. The main content area displays a deployment titled "Microsoft.Template-20251014215738 | Overview". The "Overview" tab is selected, showing deployment details: Deployment name: Microsoft.Template-20251014215738, Subscription: upgradrl-16996605801172, Resource group: upgrad-rg-azure-project, Start time: 14/10/2025, 21:57:11, Correlation ID: 74711420-ab6e-4a10-8017-e8b1995b39df. Below this, a table lists deployment details for various resources:

Resource	Type	Status	Operation
Web-LB-PIP	Public IP address	Created	Operation
RDGateway-pip	Public IP address	Created	Operation
eastus-Web-NSG	Network security group	OK	Operation
eastus2-VNet	Virtual network	Created	Operation
eastus-VNet	Virtual network	Created	Operation
eastusrsstorage	Storage account	Accepted	Operation
eastus2grsstora...	Storage account	Accepted	Operation
eastus2-WS11-NSG	Network security group	OK	Operation
backend-fw-pip	Public IP address	Created	Operation
privateling-flr...	Private DNS zone	Accepted	Operation

The right sidebar shows a "Notifications" panel with a message: "... Deployment is in progress... Deployment to resource group 'upgrad-rg-azure-project' is in progress." A timestamp indicates it was a few seconds ago. The bottom right corner shows the date and time as 10/14/2025, 9:58 PM.

## 6. Deployment Outputs

- Once succeeded → Go to Resource Group

The screenshot shows the Microsoft Azure portal interface, similar to the previous one but with different notification content. The deployment status has changed to "Deployment succeeded". The notifications panel now displays: "Deployment 'Microsoft.Template-20251014215738' to resource group 'upgrad-rg-azure-project' was successful." It includes two buttons: "Pin to dashboard" and "Go to resource group". The "Go to resource group" button is highlighted with a blue box. The bottom right corner shows the date and time as 10/14/2025, 10:01 PM.



## Verification

- Resource Group **upgrad-rg-azure-project** created.

Name	Type	Location
backend-firewall	Firewall	East US 2
backend-fw-pip	Public IP address	East US 2
backend-rt	Route table	East US
eastus-VNet	Virtual network	East US
eastus-Web-NSG	Network security group	East US
eastus2-VNet	Virtual network	East US 2
eastus2-WS11-NSG	Network security group	East US 2
eastus2grsstorage	Storage account	East US 2
eastus2grsstorage-pe	Private endpoint	East US 2
eastus2grsstorage-pe.nic.d652636d-dc94-4c47-bf2f-	Network interface	East US 2
eastus2rrsstorage	Storage account	East US
privatenlink.file.core.windows.net	Private DNS zone	Global

- VNets **eastus-VNet** and **eastus2-VNet** visible under **Virtual networks**.

Name	Resource group	Location	Subscription
eastus-VNet	upgrad-rg-azure-project	East US	npupgradl-1696605801172
eastus2-VNet	upgrad-rg-azure-project	East US 2	npupgradl-1696605801172

- **Subnets** (`websubnet`, `RDGatewaySubnet`, `GatewaySubnet`) correctly created in `eastus-VNet`

**eastus-VNet | Subnets**

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
websubnet	10.0.1.0/24	-	249	-	-	-
RDGatewaySubnet	10.0.2.0/24	-	250	-	-	-
GatewaySubnet	10.0.255.0/27	-	1	availability ...	-	-

- **Subnets** (`appsubnet`, `AzureFirewallSubnet`, `GatewaySubnet`) correctly created in `eastus2-VNet`

**eastus2-VNet | Subnets**

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
GatewaySubnet	10.1.255.0/27	-	1	availability ...	-	-
AzureFirewallSubnet	10.1.254.0/26	-	56	-	-	-
appsubnet	10.1.1.0/24	-	249	-	-	backend-rt

# Task II — Deploy Virtual Machines

## Objective

Deploy web servers, RD Gateway, and WS11 backend server with high availability.

## Steps

### 1. Verify Availability Set

- Portal → Availability sets → Web-AvailabilitySet.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (with 'All resources (Resource Manager)' selected), 'Resource groups (Resource Manager)', 'App Services', 'Function App', 'Azure SQL Database (Azure SQL)', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Microsoft Entra ID', 'Monitor', 'Advisor', 'Microsoft Defender for Cloud', and 'Cost Management + Billing'. The search bar at the top contains 'portal.azure.com/#/npupgradelabs.onmicrosoft.com/resource/subscriptions/61659804-c992-4721-abe0-6968b4b0d265/resourceGrou...'. The main content area displays the 'Availability sets' blade for 'Web-AvailabilitySet'. The 'Overview' section shows the following details:

Resource group (move)	ugrgrad-rg-azure-project	Fault domains	2
Location	East US	Update domains	5
Subscription (move)	npupgradelabs-1696005081172	Virtual machines	2
Subscription ID	61659804-c992-4721-abe0-6968b4b0d265	Managed	Yes
		Colocation status	N/A

The 'Virtual machines' section lists two VMs:

Name	Status	Colocation status	Fault Domain	Update Domain
w1	Running	1	1	
w2	Running	0	0	

## 2. Confirm Virtual Machines

- w1, w2, RDGateway, WS11 visible in Virtual Machines.

RDGateway →

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes 'Compute infrastructure' under 'Virtual machines'. The main content area displays the 'RDGateway' virtual machine details. The 'Overview' tab is selected, showing the VM's status as 'Running' in 'East US'. The 'Essentials' section provides detailed information such as the operating system (Windows Server 2019 Datacenter), size (Standard B1ms), and public IP address (172.160.47.73). Other tabs like 'Properties', 'Monitoring', and 'Capabilities' are also visible.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes 'Compute infrastructure' under 'Virtual machines'. The main content area displays the 'RDGateway' virtual machine details. A modal window titled 'Add inbound security rule' is open, showing the configuration for a new network security group rule. The 'Destination' is set to 'Any', 'Service' to 'Custom', and 'Protocol' to 'TCP'. The 'Destination port ranges' is set to '443'. The 'Action' is set to 'Allow'. The 'Priority' is set to '101', and the 'Name' is set to 'Allow-HTTPS-RDGateway'. The 'Description' field contains the note 'Allow inbound HTTPS (RDP over SSL) for RD Gateway access'. The bottom right corner of the modal has a note: 'Go to Settings to activate Windows Firewall'.

**W1 →**

The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons. The main area is titled "Compute infrastructure | Virtual machines". A sub-menu for "Virtual machines" is open, showing a list of VMs: RDGateway, w1, w2, and WS11. The "w1" item is selected and highlighted with a blue border. On the right, the "Overview" tab of the "w1" VM's details page is displayed. The "Essentials" section includes information such as Resource group ([move](#)), Status (Running), Location (East US), Subscription ([move](#)), and Time created (14/10/2025, 16:27 UTC). The "Networking" tab is also visible.

**W2 →**

This screenshot is nearly identical to the one above, showing the Microsoft Azure portal. The left sidebar and main navigation bar are the same. The "Virtual machines" sub-menu is open, and "w2" is selected. The "Overview" tab of the "w2" VM's details page is shown on the right. The "Essentials" section provides similar information: Resource group ([move](#)), Status (Running), Location (East US), Subscription ([move](#)), and Time created (14/10/2025, 16:27 UTC). The "Networking" tab is present but not active.

## WS11 →

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service links like Home, Dashboard, All services, and Favorites. Under Favorites, 'All resources (Resource Manager)' is selected. The main content area is titled 'Compute infrastructure | Virtual machines' and shows a list of virtual machines. One VM, 'WS11', is highlighted. The right pane displays detailed information about 'WS11', including its operating system (Windows Server 2019 Datacenter), size (Standard\_B1ms), and location (East US 2). It also shows the subscription ID and creation date.

Name	Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address	Disks
RDGateway	npupgradl-169...	upgrad-rg-azur...	East US	Running	Windows	Standard_B1ms	172.190.47.75	1
w1	npupgradl-169...	upgrad-rg-azur...	East US	Running	Windows	Standard_B1ms	4.246.183.50	1
w2	npupgradl-169...	upgrad-rg-azur...	East US	Running	Windows	Standard_B1ms	4.246.183.50	1
WS11	npupgradl-169...	upgrad-rg-azur...	East US 2	Running	Windows	Standard_B1ms	-	1

## Virtual Machines →

The screenshot shows the Microsoft Azure portal interface, similar to the previous one but with a different focus. The left sidebar shows the same navigation options. The main content area is titled 'Compute infrastructure | Virtual machines' and displays a grid of all virtual machines in the account. The columns include Name, Subscription, Resource Group, Location, Status, Operating system, Size, Public IP address, and Disks. The 'Subscription equals all' filter is applied.

Name	Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address	Disks
RDGateway	npupgradl-169...	upgrad-rg-azur...	East US	Running	Windows	Standard_B1ms	172.190.47.75	1
w1	npupgradl-169...	upgrad-rg-azur...	East US	Running	Windows	Standard_B1ms	4.246.183.50	1
w2	npupgradl-169...	upgrad-rg-azur...	East US	Running	Windows	Standard_B1ms	4.246.183.50	1
WS11	npupgradl-169...	upgrad-rg-azur...	East US 2	Running	Windows	Standard_B1ms	-	1

### 3. Check VNet Peering

- **eastUS-VNet → Peerings → Confirm “Connected” to eastUS2-VNet.**

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes options like Home, Dashboard, All services, and a Favorites section with items such as All resources (Resource Manager), Resource groups (Resource Manager), App Services, Function App, Azure SQL Database (Azure SQL), Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Microsoft Entra ID, Monitor, Advisor, Microsoft Defender for Cloud, and Cost Management + Billing. The main content area is titled "eastus-VNet | Peerings" and displays a table of peerings. The table has columns for Name, Peering sync status, Peering state, Remote VNet, Virtual network, and Cross-tenant. One entry, "PeeringToeastus2", is listed with a green checkmark in the Peering sync status column, indicating "Fully Synchronized", and a green checkmark in the Peering state column, indicating "Connected". The status for the Remote VNet is "eastus2-VNet", and the status for the Virtual network is "Disabled". The bottom right corner of the screen shows the date and time as 10/14/2025 at 10:23 PM.

- Vice versa eastUS2-VNet → Peerings → Confirm “Connected” to eastus-VNet

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes options like Home, Dashboard, All services, and a Favorites section with items such as All resources (Resource Manager), Resource groups (Resource Manager), App Services, Function App, Azure SQL Database (Azure SQL), Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Microsoft Entra ID, Monitor, Advisor, Microsoft Defender for Cloud, and Cost Management + Billing. The main content area is titled "eastus2-VNet | Peerings" and displays a table of peerings. The table has columns for Name, Peering sync status, Peering state, Remote VNet, Virtual network, and Cross-tenant. One entry, "PeeringToeastus", is listed with a green checkmark in the Peering sync status column, indicating "Fully Synchronized", and a green checkmark in the Peering state column, indicating "Connected". The status for the Remote VNet is "eastus-VNet", and the status for the Virtual network is "Disabled". The bottom right corner of the screen shows the date and time as 10/14/2025 at 10:25 PM.

## Verification

- W1 and W2 deployed in EastUS under availability set. → Done above
- RDGateway has public IP. → Done above
- WS11 deployed in EastUS2 (private IP only). → Done above
- Peering between VNets connected. → Done above

---

## Task III — Implement Secure Connectivity

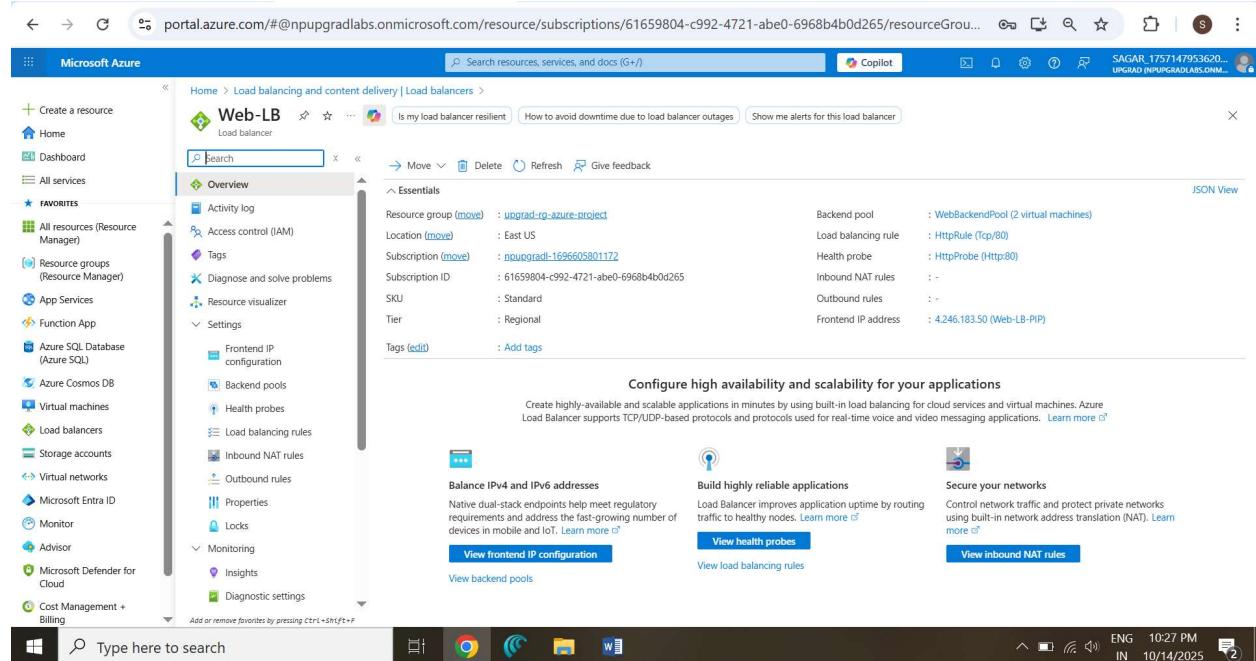
### Objective

Establish secure access and restricted communication using NSGs, VPN/Private Link, and Load Balancer.

### Steps

#### 1. Load Balancer Configuration

- Portal → Load Balancers → Web-LB.



The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes options like Home, Dashboard, All services, Favorites (with items like All resources (Resource Manager), Resource groups (Resource Manager), App Services, Function App, Azure SQL Database (Azure SQL), Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Microsoft Entra ID, Monitor, Advisor, Microsoft Defender for Cloud, and Cost Management + Billing). The main content area is titled "Web-LB" under "Load balancing and content delivery | Load balancers". The "Overview" tab is selected. The "Essentials" section displays the following details:

Setting	Value
Resource group (move)	: upgrad-rg-azure-project
Location (move)	: East US
Subscription (move)	: npupgradl-1696605801172
Subscription ID	: 61659804-c992-4721-abe0-6968b4b0d265
SKU	: Standard
Tier	: Regional
Tags (edit)	: Add tags
Backend pool	: WebBackendPool (2 virtual machines)
Load balancing rule	: HttpRule (Tcp:80)
Health probe	: HttpProbe (Http:80)
Inbound NAT rules	: -
Outbound rules	: -
Frontend IP address	: 4246.183.50 (Web-LB-PIP)

Below the essentials section, there's a callout for "Configure high availability and scalability for your applications" with links to "Balance IPv4 and IPv6 addresses", "Build highly reliable applications", and "Secure your networks". At the bottom of the overview page, there are buttons for "View frontend IP configuration", "View health probes", "View load balancing rules", and "View inbound NAT rules".

- Verify Frontend IP, Backend Pool, and Health Probe.

The screenshot shows the Azure portal interface for managing a load balancer. The left sidebar navigation bar includes options like Home, Dashboard, All services, Favorites, and various Azure services. The main content area is titled "Web-LB | Frontend IP configuration". It displays a table with one item: "LoadBalancerFrontEnd" with IP address 4.246.183.50 (Web-LB-PIP) and 1 rule. A sidebar on the left provides navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, and Settings (which is currently selected). The status bar at the bottom shows system information: ENG IN 10:28 PM 10/14/2025.

The screenshot shows the Azure portal interface for managing a load balancer. The left sidebar navigation bar includes options like Home, Dashboard, All services, Favorites, and various Azure services. The main content area is titled "Web-LB | Backend pools". It displays a table with two items: "WebBackendPool (2)". The first item is "WebBackendPool" with resource name w2, IP address 10.0.1.4, network interface w2-nic, and 1 rule. The second item is "WebBackendPool" with resource name w1, IP address 10.0.1.5, network interface w1-nic, and 1 rule. A sidebar on the left provides navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, and Settings (which is currently selected). The status bar at the bottom shows system information: ENG IN 10:29 PM 10/14/2025.

## Health Probe :

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, and Favorites (which includes All resources (Resource Manager), Resource groups (Resource Manager), App Services, Function App, Azure SQL Database (Azure SQL), Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Microsoft Entra ID, Monitor, Advisor, Microsoft Defender for Cloud, and Cost Management + Billing). The main content area is titled "Web-LB | Health probes" and shows an "Overview" section with a search bar and a table of health probe details. The table has columns for Name, Protocol, Port, Path, and Used By. One entry, "HttpProbe", is listed with Http as the protocol, port 80, path /, and used by "HttpRule". Below the table are sections for "Access control (IAM)", "Tags", "Diagnose and solve problems", "Resource visualizer", and "Settings" (which includes Frontend IP configuration, Backend pools, and Health probes). The "Health probes" section is currently selected. At the bottom of the page, there are links for "Add", "Refresh", and "Give feedback". The status bar at the bottom right shows the user's name (SAGAR\_1757147953620\_UPGRAD (NPUPGRADLABS.DRM...)), the date (10/14/2025), and the time (10:30 PM).

## 2. Network Security Groups (NSGs)

- EastUS-Web-NSG allow HTTPS (443), RDP (3389).

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, and Favorites (which includes All resources (Resource Manager), Resource groups (Resource Manager), App Services, Function App, Azure SQL Database (Azure SQL), Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Microsoft Entra ID, Monitor, Advisor, Microsoft Defender for Cloud, and Cost Management + Billing). The main content area is titled "eastus-Web-NSG | Network security groups" and shows an "Overview" section with a search bar and a table of security rule details. The table has columns for Priority, Name, Port, Protocol, Source, Destination, and Action. There are two sections: "Inbound Security Rules" and "Outbound Security Rules". In the "Inbound Security Rules" section, rules include AllowHTTPS (Priority 100, Port 443, Protocol Tcp, Any, Any, Allow), AllowRDP (Priority 200, Port 3389, Protocol Tcp, Any, Any, Allow), AllowVnetInBound (Priority 65000, Port Any, Protocol Any, VirtualNetwork, VirtualNetwork, Allow), AllowAzureLoadBalancer (Priority 65001, Port Any, Protocol Any, AzureLoadBalancer, Any, Allow), and DenyAllInBound (Priority 65500, Port Any, Protocol Any, Any, Any, Deny). In the "Outbound Security Rules" section, rules include AllowVnetOutBound (Priority 65000, Port Any, Protocol Any, VirtualNetwork, VirtualNetwork, Allow), AllowInternetOutBound (Priority 65001, Port Any, Protocol Any, Internet, Any, Allow), and DenyAllOutBound (Priority 65500, Port Any, Protocol Any, Any, Any, Deny). The status bar at the bottom right shows the user's name (SAGAR\_1757147953620\_UPGRAD (NPUPGRADLABS.DRM...)), the date (10/14/2025), and the time (10:33 PM).

- **EastUS2-WS11-NSG deny outbound to social media sites.**

**Overview**

**Essentials**

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowAdmin	3389	Tcp	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
4096	DenyOutboundAll	Any	Any	Any	0.0.0.0/0	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

### 3. Secure Communication

- Confirm encrypted traffic between VNets.

**PeeringToeastus**

**Local virtual network summary**

**Local virtual network peering settings**

Allow 'eastus2-VNet' to access 'eastus-VNet'	<input checked="" type="checkbox"/>
Allow 'eastus2-VNet' to receive forwarded traffic from 'eastus-VNet'	<input checked="" type="checkbox"/>
Allow gateway or route server in 'eastus2-VNet' to forward traffic to 'eastus-VNet'	<input type="checkbox"/>
Enable 'eastus2-VNet' to use 'eastus-VNet's remote gateway or route server	<input type="checkbox"/>

## 4. Azure Private Link Verification

Microsoft Azure

eastus2grsstorage-pe

Private endpoint

Search resources, services, and docs (G+)

Copilot

SAGAR\_1757147953620...  
UPGRAD (NPUPGRADLABS.ONMICROSOFT.COM)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Application security groups

DNS configuration

Properties

Locks

Monitoring

Insights

Alerts

Metrics

Automation

CLI / PS

Tasks

Resource group (move) : upgrad-rg-azure-project

Location : East US 2

Subscription (move) : npupgrad-1696605801172

Subscription ID : 61659804-c992-4721-abe0-6968b4b0d265

Provisioning state : Succeeded

Virtual network/subnet : eastus2-VNet/appsubnet

Network interface : eastus2grsstorage-pe-nic-d652636d-dc94-4c47-bf2f-5f3f21d9fd2d

Private link resource : eastus2grsstorage

Target sub-resource : file

Connection status : Approved

Request/Response : Auto-Approved

Tags (edit) : Add tags

Add or remove favorites by pressing Ctrl+Shift+F

Type here to search

Give feedback

ENG 11:34 PM IN 10/14/2025

## Verification

- LB public IP reachable.

Not secure 20.189.162.73

Windows Server

Internet Information Services

Welcome Bienvenue Tervetuloa

ようこそ Benvenuto 歓迎

Bem-vindo

Viteje

Καλώς ορίσατε

Willkommen

Velkommen

Microsoft

Activate Windows  
Go to Settings to activate Windows.

Type here to search

Give feedback

ENG 2:01 AM IN 10/15/2025

- w1 & w2 appear in backend pool.

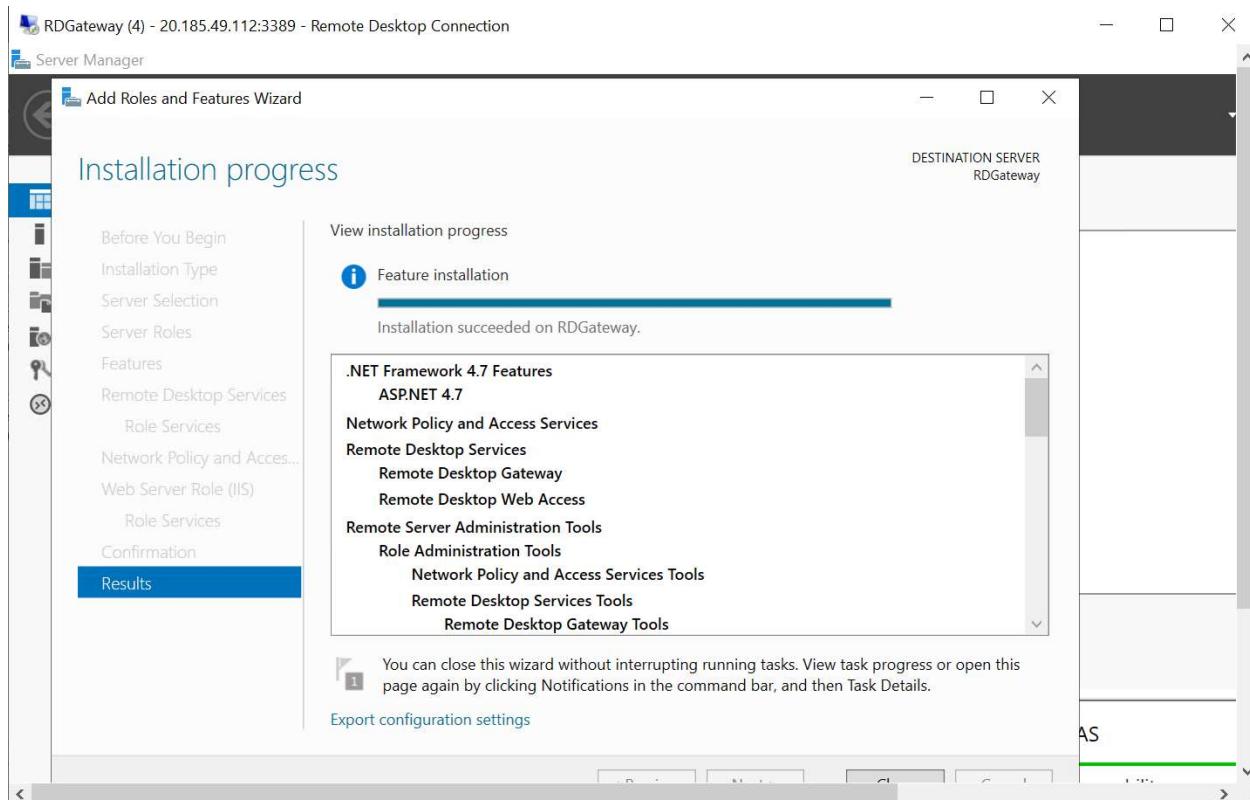
The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Home, Dashboard, All services, and Load balancers. The main content area is titled "Web-LB | Backend pools" and shows a table of backend pools. The table has columns: Backend pool, Resource Name, IP address, Network interface, Availability zone, Rules count, Resource Status, and Admin state. There are two entries under "WebBackendPool (2)":

Backend pool	Resource Name	IP address	Network interface	Availability zone	Rules count	Resource Status	Admin state
WebBackendPool	w2	10.0.1.4	w2-nic	-	1	-	None
WebBackendPool	w1	10.0.1.5	w1-nic	-	1	-	None

# RD Gateway & RD Web Access — GUI-based Setup (Windows Server 2022/2025)

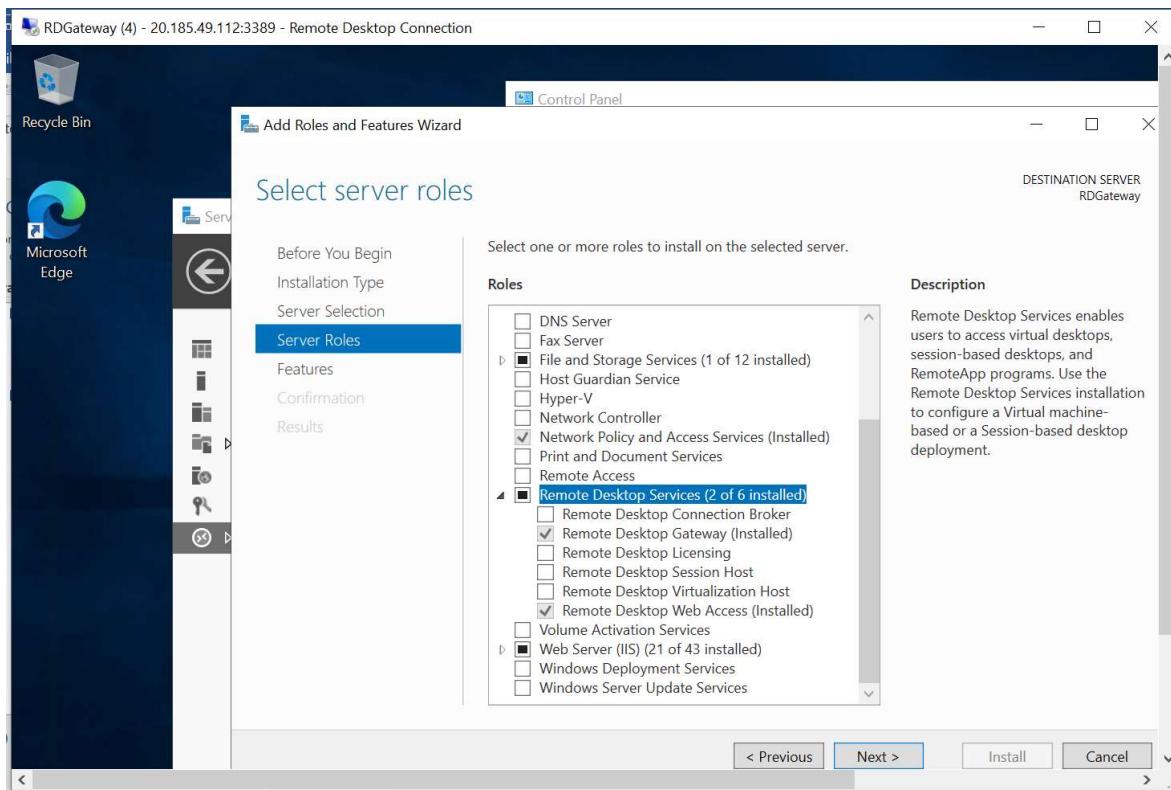
## • STEP 1 — Install Roles via Server Manager

1. Open **Server Manager** → **Manage** → **Add Roles and Features**.
2. Choose **Role-based or feature-based installation**, click **Next**.
3. Select **This server**.
4. In **Server Roles**, check:
  - **Remote Desktop Gateway**
  - **Remote Desktop Web Access**
  - IIS and Management Tools will auto-select → keep them.
5. Click **Next** until **Install**.
6. Wait for installation to complete → **Close**.



## • STEP 2 — Verify Roles Installed

- Open **Server Manager** → **Dashboard** → **Remote Desktop Services**.
- You should see **RD Gateway** and **RD Web Access** listed.
- Optionally, open **Programs and Features** → **Turn Windows features on/off** to confirm.



## • STEP 3 — Create a Valid HTTPS Certificate

You can use **IIS Manager** or **Certificates MMC**. Using **Powershell**

# --- Step 3: Create self-signed certificate

```
$publicName = (Invoke-RestMethod -Uri "https://ifconfig.me/ip" -ErrorAction SilentlyContinue)

if (-not $publicName) { $publicName = (hostname) }
Write-Host "Creating self-signed certificate for $publicName..." -ForegroundColor Cyan
$cert = New-SelfSignedCertificate `

-DnsName $publicName `

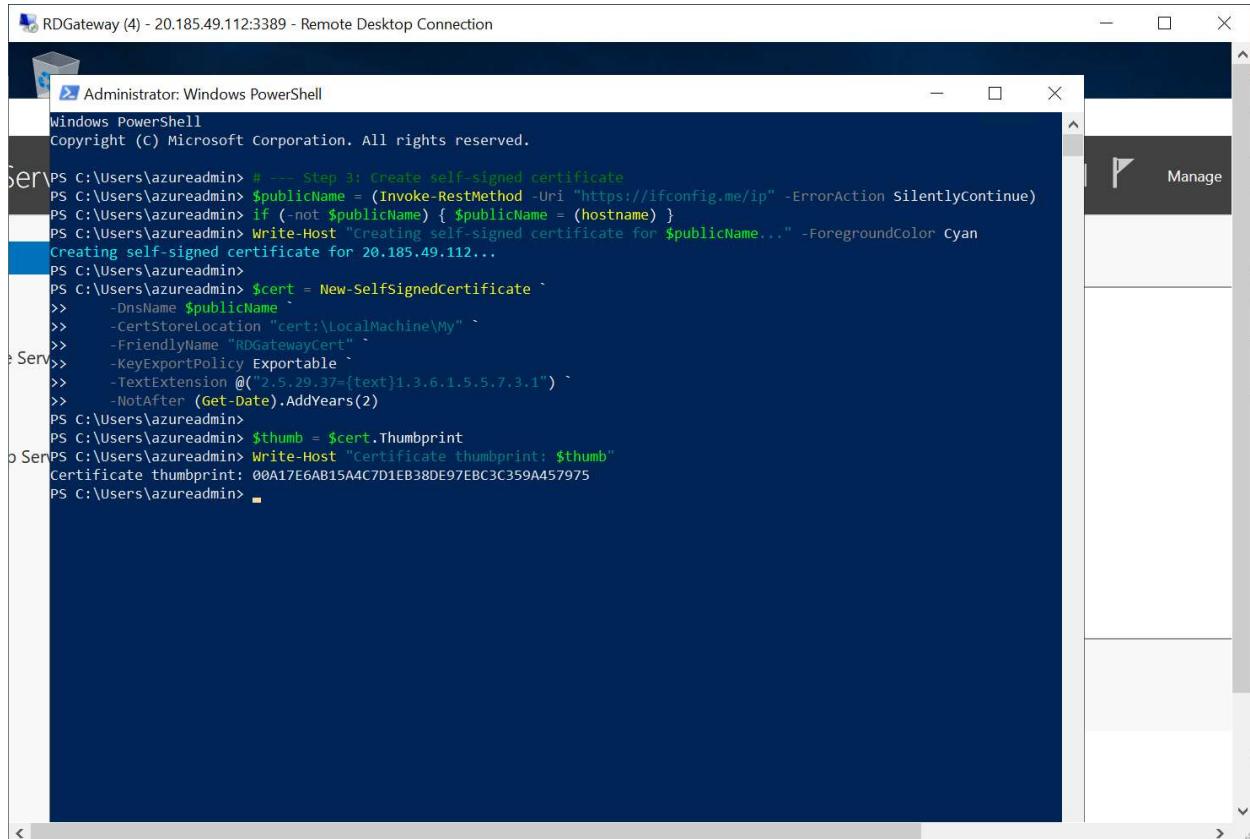
-CertStoreLocation "cert:\LocalMachine\My" `

-FriendlyName "RDGatewayCert" `

-KeyExportPolicy Exportable `

-TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1") `

-NotAfter (Get-Date).AddYears(2)
$thumb = $cert.Thumbprint
Write-Host "Certificate thumbprint: $thumb"
```



```
Administrator: Windows PowerShell
Windows PowerShell
copyright (c) Microsoft Corporation. All rights reserved.

PS C:\Users\azureadmin> # --- Step 3: Create self-signed certificate
PS C:\Users\azureadmin> $publicName = (Invoke-RestMethod -Uri "https://ifconfig.me/ip" -ErrorAction SilentlyContinue)
PS C:\Users\azureadmin> if (-not $publicName) { $publicName = (hostname) }
PS C:\Users\azureadmin> Write-Host "Creating self-signed certificate for $publicName..." -ForegroundColor Cyan
Creating self-signed certificate for 20.185.49.112...
PS C:\Users\azureadmin>
PS C:\Users\azureadmin> $cert = New-SelfSignedCertificate `

    >> -DnsName $publicName `

    >> -CertStoreLocation "cert:\LocalMachine\My" `

    >> -FriendlyName "RDGatewayCert" `

    >> -KeyExportPolicy Exportable `

    >> -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1") `

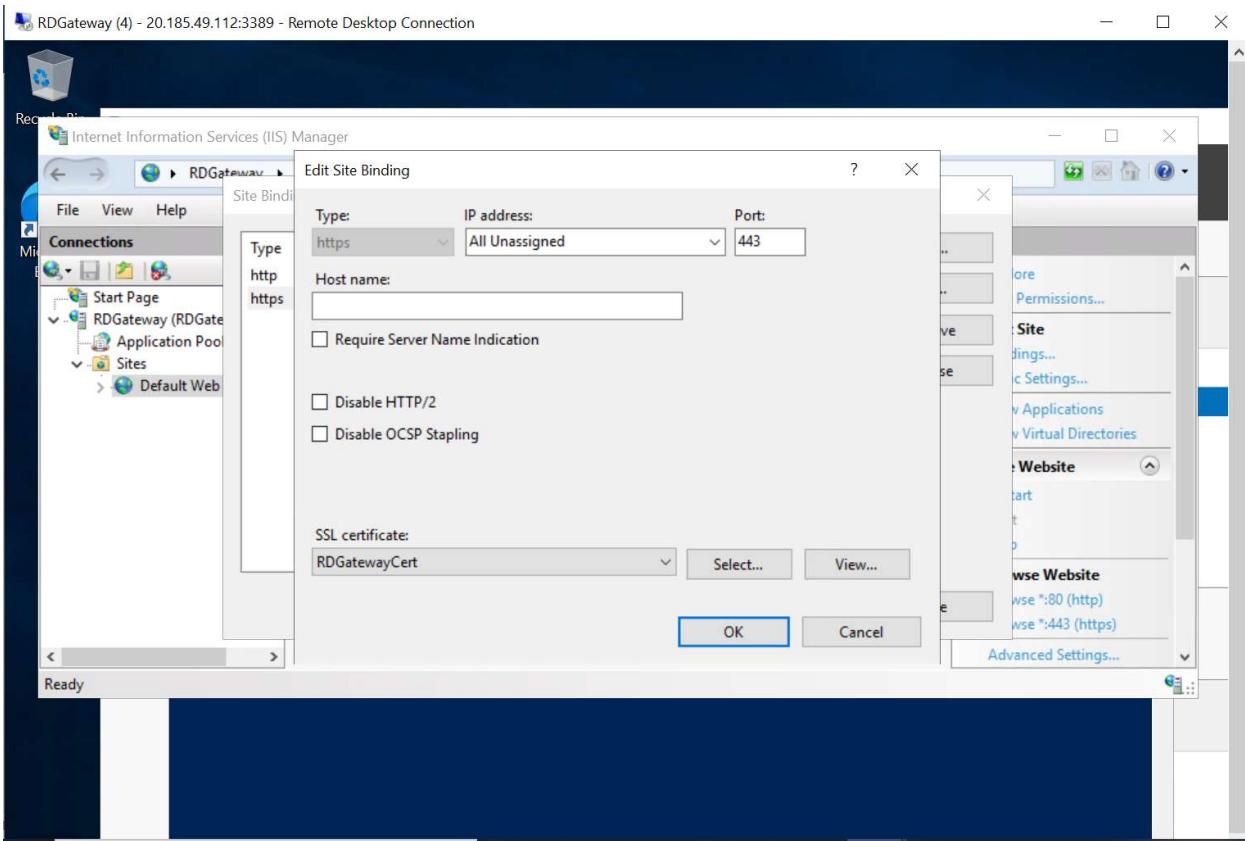
    >> -NotAfter (Get-Date).AddYears(2)
PS C:\Users\azureadmin> $thumb = $cert.Thumbprint
PS C:\Users\azureadmin> Write-Host "Certificate thumbprint: $thumb"
Certificate thumbprint: 00A17E6AB15A4C7D1EB38DE97EBC3C359A457975
PS C:\Users\azureadmin>
```

- **IIS Manager**

1. Open **IIS Manager** → click server name (left pane).
2. Double-click **Server Certificates** (center).
3. In right Actions pane → click **Create Self-Signed Certificate**.
4. Name it: RDGW-SelfSigned-20.185.49.112.
5. Choose **Personal** store → OK.

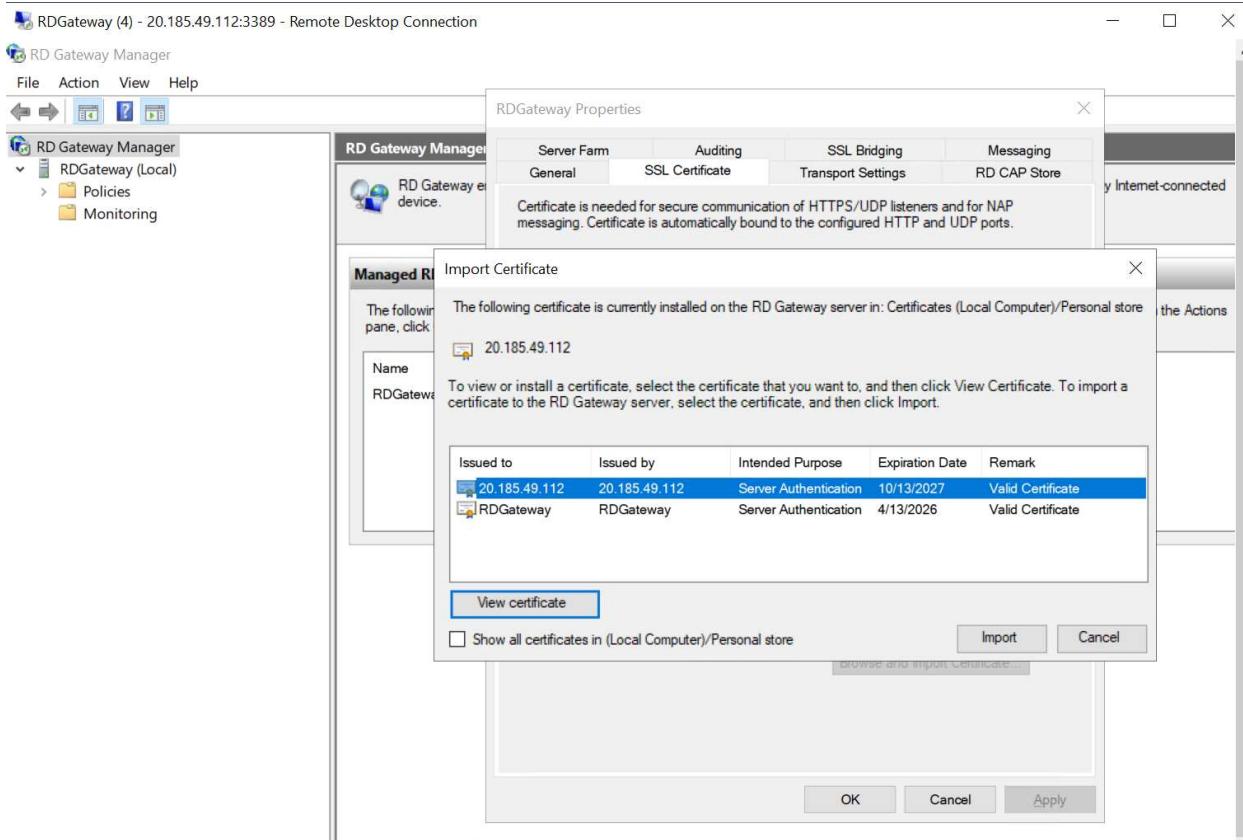
- **STEP 4 — Bind Certificate to IIS (HTTPS 443)**

1. In **IIS Manager** → expand **Sites** → **Default Web Site**.
2. Right pane → click **Bindings....**
3. Click **Add...** →
  - Type: https
  - IP address: All Unassigned or your public IP
  - Port: 443
  - SSL certificate: choose the cert you just created
  - Click **OK** → then **Close**.



- **STEP 5 — Bind Certificate to RD Gateway**

1. Open **RD Gateway Manager** (`tsgateway.msc`).
2. Right-click server name → **Properties**.
3. Go to **SSL Certificate** tab.
4. Click **Import a certificate into the personal store**.
5. Select your certificate → click **Import**.
6. Once imported, select it and click **Apply**.



- **STEP 6 — Configure Firewall Rules (if needed)**

Windows usually enables these automatically.

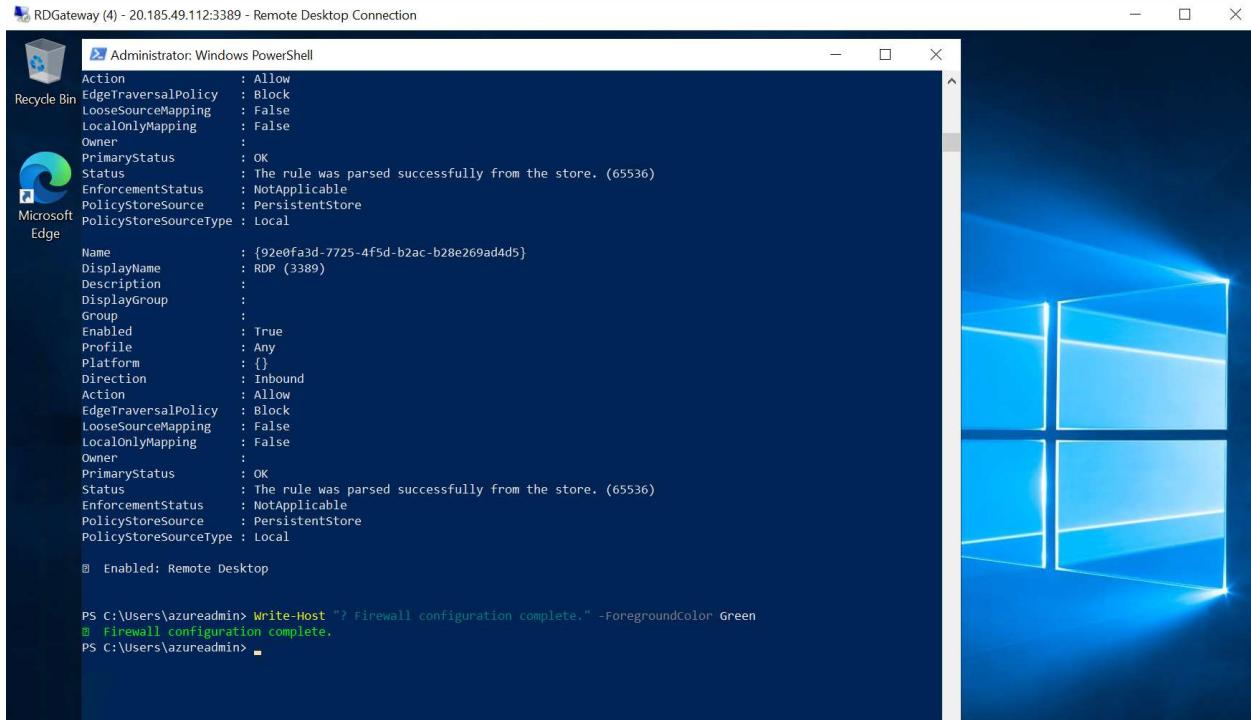
To verify:

1. Open **Windows Defender Firewall** → **Advanced settings**.
2. Click **Inbound Rules** → scroll to:
  - *World Wide Web Services (HTTP and HTTPS)*
  - *Remote Desktop Gateway*
3. Make sure **Enabled = Yes** and **Action = Allow**.

If not → right-click → **Enable Rule**.

## Powershell Script →

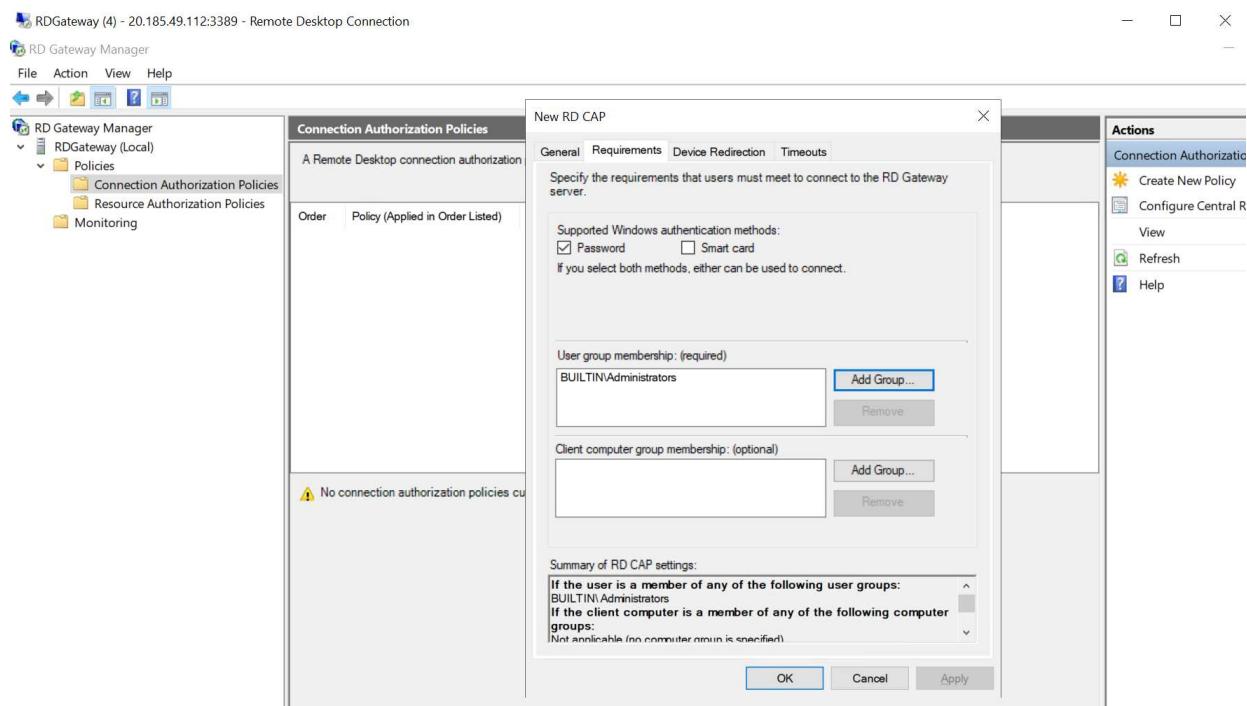
```
Write-Host "==== Enabling RD Gateway Firewall Rules ===" -ForegroundColor Cyan
$rules= @("World Wide Web Services (HTTP)", "World Wide Web Services (HTTPS)", "Remote Desktop Gateway", "Remote Desktop")
foreach($r in $rules){
    try{Enable-NetFirewallRule -DisplayGroup $r -ErrorAction Stop; Write-Host "✓ Enabled: $r"}
    catch{if($r -match "HTTP" -and $r -notmatch "HTTPS"){New-NetFirewallRule -DisplayName "HTTP (80)" -Dir In -Protocol TCP -LocalPort 80 -Action Allow}
        elseif($r -match "HTTPS"){New-NetFirewallRule -DisplayName "HTTPS (443)" -Dir In -Protocol TCP -LocalPort 443 -Action Allow}
        elseif($r -match "Desktop"){New-NetFirewallRule -DisplayName "RDP (3389)" -Dir In -Protocol TCP -LocalPort 3389 -Action Allow}}
    Write-Host "✓ Firewall configuration complete." -ForegroundColor Green
```



## • STEP 7 — Configure CAP and RAP (Access Policies)

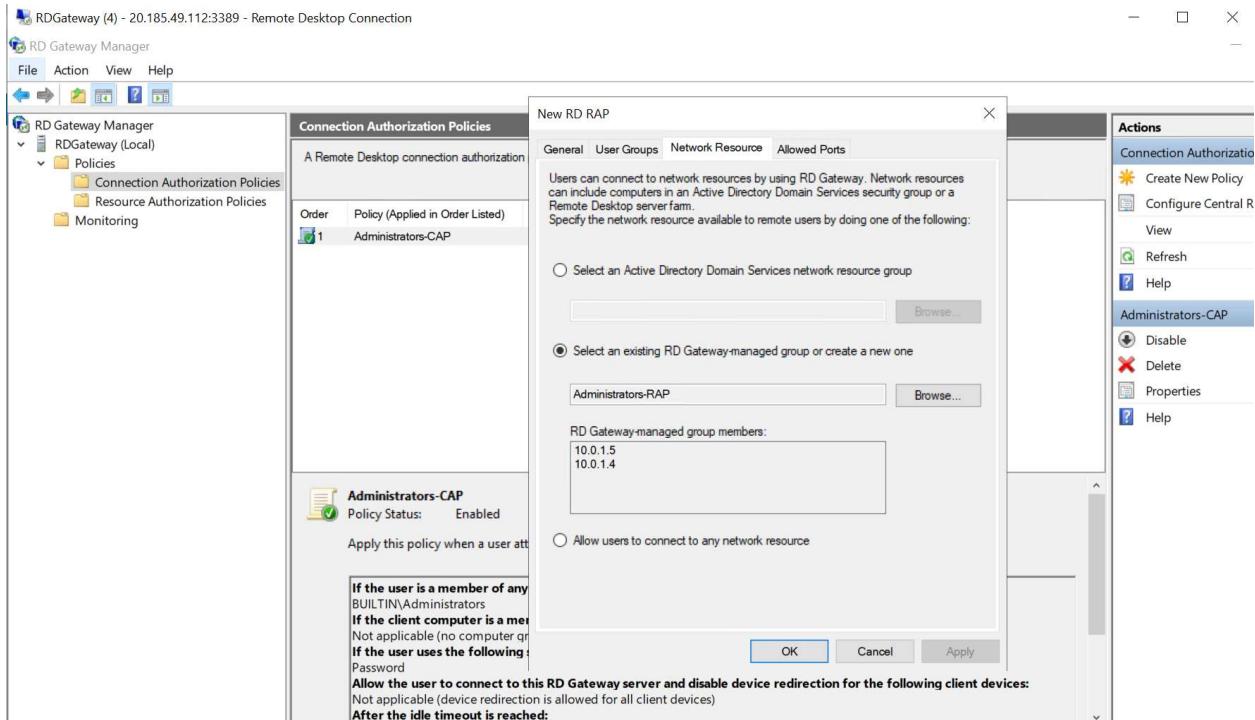
1. In RD Gateway Manager, expand your server → Policies → Connection Authorization Policies (CAP).

- Right-click → Create New Policy.
- Name: **Administrators-CAP**.
- Choose User Group: **Administrators**.
- Click **Finish**.



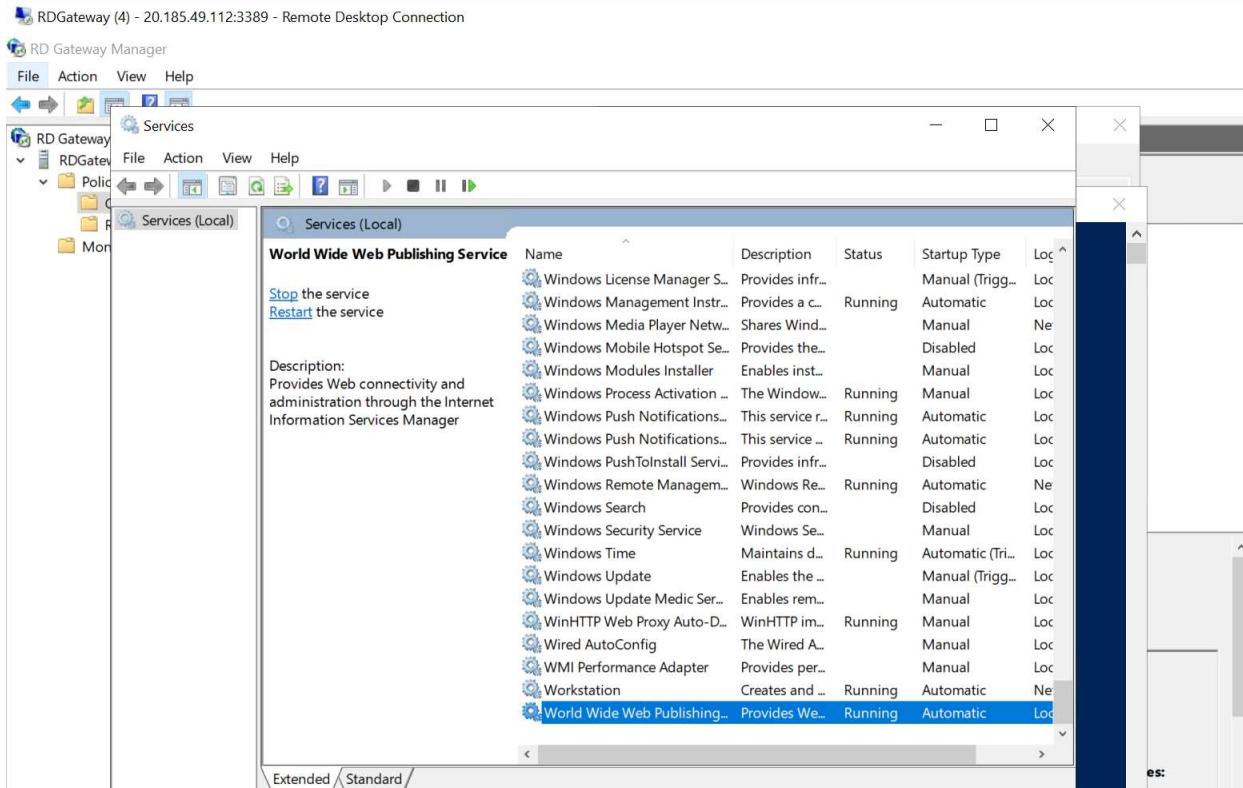
## 2. Expand Resource Authorization Policies (RAP) →

- Right-click → **Create New Policy.**
- Name: Administrators-RAP.
- Add **Computer Group** → add w1, w2, WS11 or any internal servers.
- Click Finish.



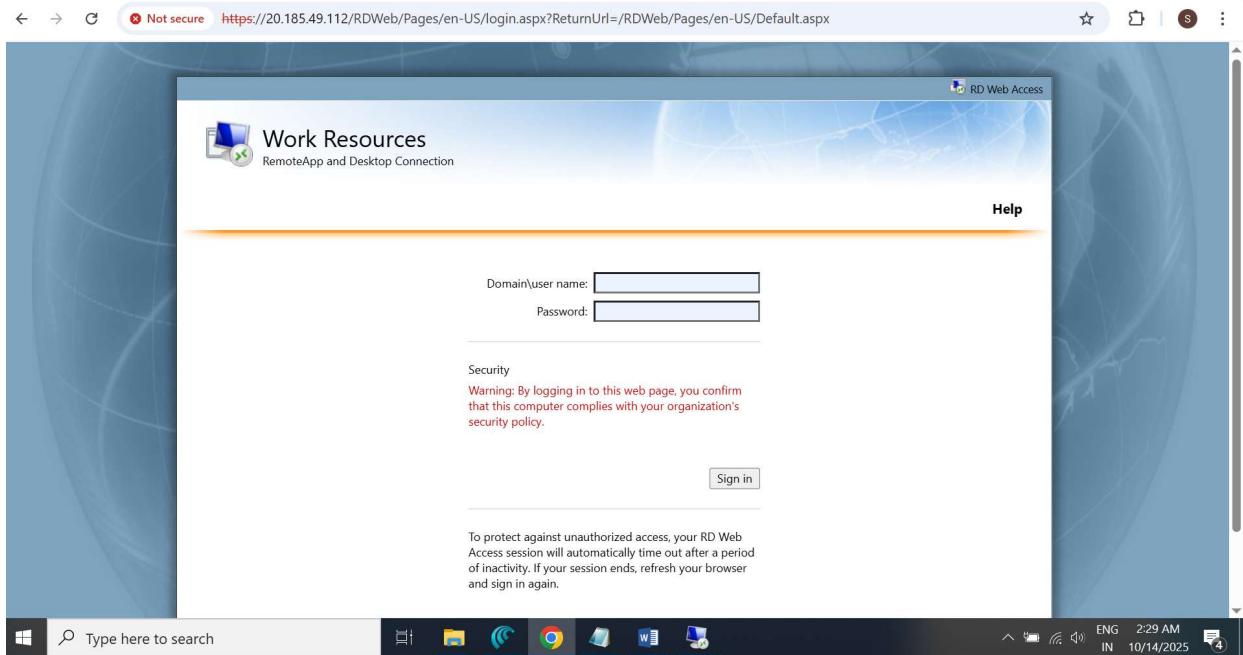
## • STEP 8 — Restart Services

1. Open **Services.msc**.
2. Locate and restart:
  - *World Wide Web Publishing Service (W3SVC)*
  - *Remote Desktop Gateway (TSGateway)*
3. Wait until **Status = Running**.



- **STEP 9 — Test the RD Web Portal**

1. Open a browser on the same server or remote client.
2. Navigate to
3. <https://20.185.49.112/RDWeb>
4. If it shows a certificate warning → click **Continue to site** (it's self-signed).
5. You should see **RD Web Access login page**.



- LOGIN →

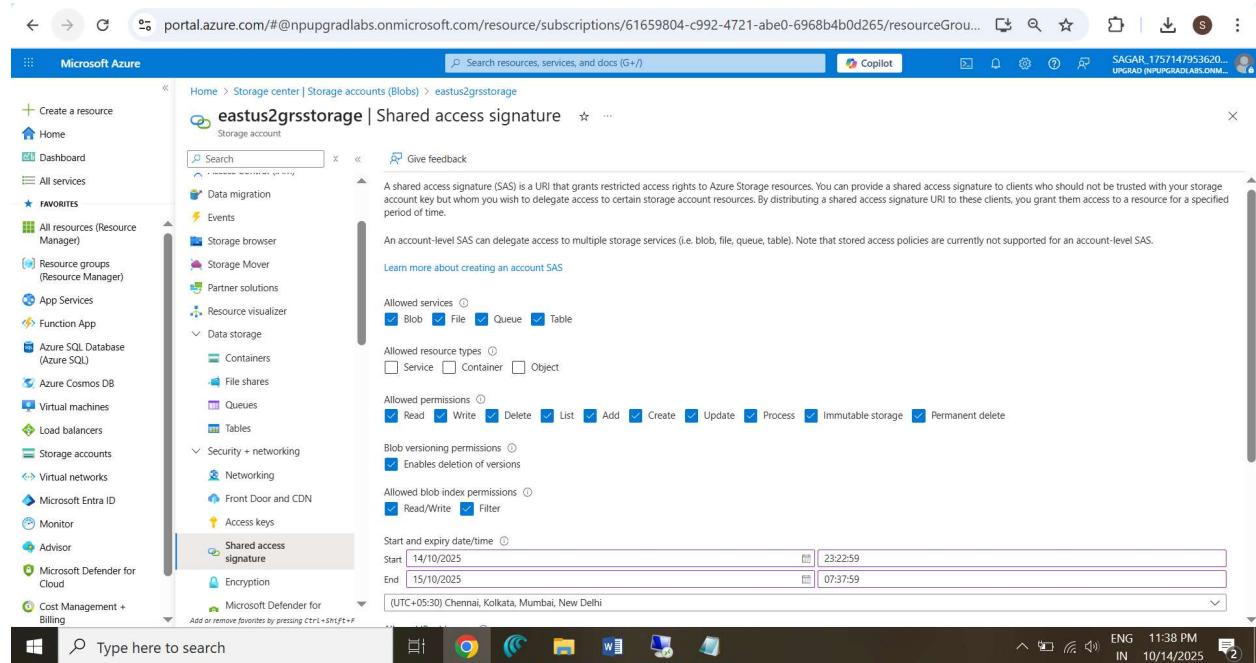
# Task IV — Setup Storage Solutions & Verification

## Objective

Deploy resilient storage, map file share, and verify connectivity.

## Steps

- Shared Access Signature (SAS)
- SAS = temporary, restricted access token generated from your storage account.



The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes Home, Dashboard, All services, and Favorites. Under Favorites, there are links for All resources (Resource Manager), Resource groups (Resource Manager), App Services, Function App, Azure SQL Database (Azure SQL), Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Microsoft Entra ID, Monitor, Advisor, Microsoft Defender for Cloud, and Cost Management + Billing. The main content area displays the 'Storage center | Storage accounts (Blobs)' section for the storage account 'eastus2grsstorage'. The 'Shared access signature' blade is open, showing configuration options for Allowed services (Blob, File, Queue, Table) and Allowed resource types (Containers, File shares, Queues, Tables). It also includes sections for Blob versioning permissions (Enables deletion of versions), Allowed blob index permissions (Read/Write, Filter), and Start and expiry date/time (Start: 14/10/2025, End: 15/10/2025, Duration: 23:22:59 to 07:37:59). The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time (10/14/2025, 11:38 PM).

- Access Keys Verification
- Access keys = full admin access for storage

**Storage account name:** eastus2grsstorage

**key1** (Rotated key) Last rotated: 14/10/2025 (0 days ago)

**key2** (Rotated key) Last rotated: 14/10/2025 (0 days ago)

- Role-Based Access Control (RBAC) Verification
- RBAC = identity-based access via Azure AD roles.

Name	Type	Role	Scope	Condition
Owner (3)				
Foreign Principal for 'QIT S...	Foreign group	Owner	Subscription (Inherited)	None
npupgradelabs-app	Service principal	Owner	Subscription (Inherited)	None
SAGAR	User	Owner	Subscription (Inherited)	None
Management Group Contributor (1)				
UpGrad Azure	User	Management Group Contributor	Management group (Inherited)	None
Storage Blob Data Contributor (3)				
SAGAR	User	Storage Blob Data Contributor	Resource group (Inherited)	None
SAGAR	User	Storage Blob Data Contributor	Subscription (Inherited)	None

## 1. Verify Storage Accounts

- **eastuszrsstorage → SKU = LRS.**

The screenshot shows the Azure Storage center interface for the 'eastuszrsstorage' account. The 'Overview' tab is selected. Key details include:

- Resource group (move):** upgrad-rg-azure-project
- Location:** eastus
- Subscription (move):** nougradl-1696605801172
- Subscription ID:** 61659804-c992-4721-abe0-6968b4b0d265
- Disk state:** Available
- Tags (edit):** Add tags

**Blob service** settings:

- Hierarchical namespace: Disabled
- Default access tier: Hot
- Blob anonymous access: Disabled
- Blob soft delete: Disabled
- Container soft delete: Disabled
- Versioning: Disabled
- Change feed: Disabled
- NFS v3: Disabled
- Allow cross-tenant replication: Disabled

**Security** settings:

- Require secure transfer for REST API operations: Enabled
- Storage account key access: Enabled
- Minimum TLS version: Version 1.0
- Infrastructure encryption: Disabled

**Networking** settings:

- Public network access: Enabled
- Private endpoint connections: 0
- Network routing: Microsoft network routing

System tray at the bottom right shows: ENG IN 11:11 PM 10/14/2025

- **eastus2grsstORAGE → SKU = GRS.**

The screenshot shows the Azure Storage center interface for the 'eastus2grsstORAGE' account. The 'Overview' tab is selected. Key details include:

- Resource group (move):** upgrad-rg-azure-project
- Location:** eastus2
- Primary/Secondary Loc...:** Primary: East US 2, Secondary: Central US
- Subscription (move):** nougradl-1696605801172
- Subscription ID:** 61659804-c992-4721-abe0-6968b4b0d265
- Disk state:** Primary: Available, Secondary: Available
- Tags (edit):** Add tags

**Blob service** settings:

- Hierarchical namespace: Disabled
- Default access tier: Hot
- Blob anonymous access: Disabled
- Blob soft delete: Disabled
- Container soft delete: Disabled
- Versioning: Disabled
- Change feed: Disabled
- NFS v3: Disabled
- Allow cross-tenant replication: Disabled

**Security** settings:

- Require secure transfer for REST API operations: Enabled
- Storage account key access: Enabled
- Minimum TLS version: Version 1.0
- Infrastructure encryption: Disabled

**Networking** settings:

- Public network access: Enabled
- Private endpoint connections: 1

System tray at the bottom right shows: ENG IN 11:23 PM 10/14/2025

## 2. Create File Share

- In **eastus2grsstorage** → **File shares** → **WS11Files**.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Home, Dashboard, All services, and Favorites. Under Favorites, 'All resources (Resource Manager)' is expanded, showing various Azure services. The main content area is titled 'eastus2grsstorage | File shares'. It displays 'File share settings' with identity-based access set to 'Not configured', default share-level permissions to 'Disabled', soft delete to '7 days', maximum capacity to '100 TiB', and security to 'Maximum compatibility'. A search bar at the top right allows searching by prefix (case-sensitive). Below the settings, a table lists the existing file share 'ws11files'. The table columns are Name, Modified, Access tier, and Quota. The 'ws11files' entry shows it was modified on 14/10/2025, 21:57:55, is in the 'Transaction optimized' tier, and has a quota of '100 GiB'. At the bottom of the page, there's a note about adding or removing favorites.

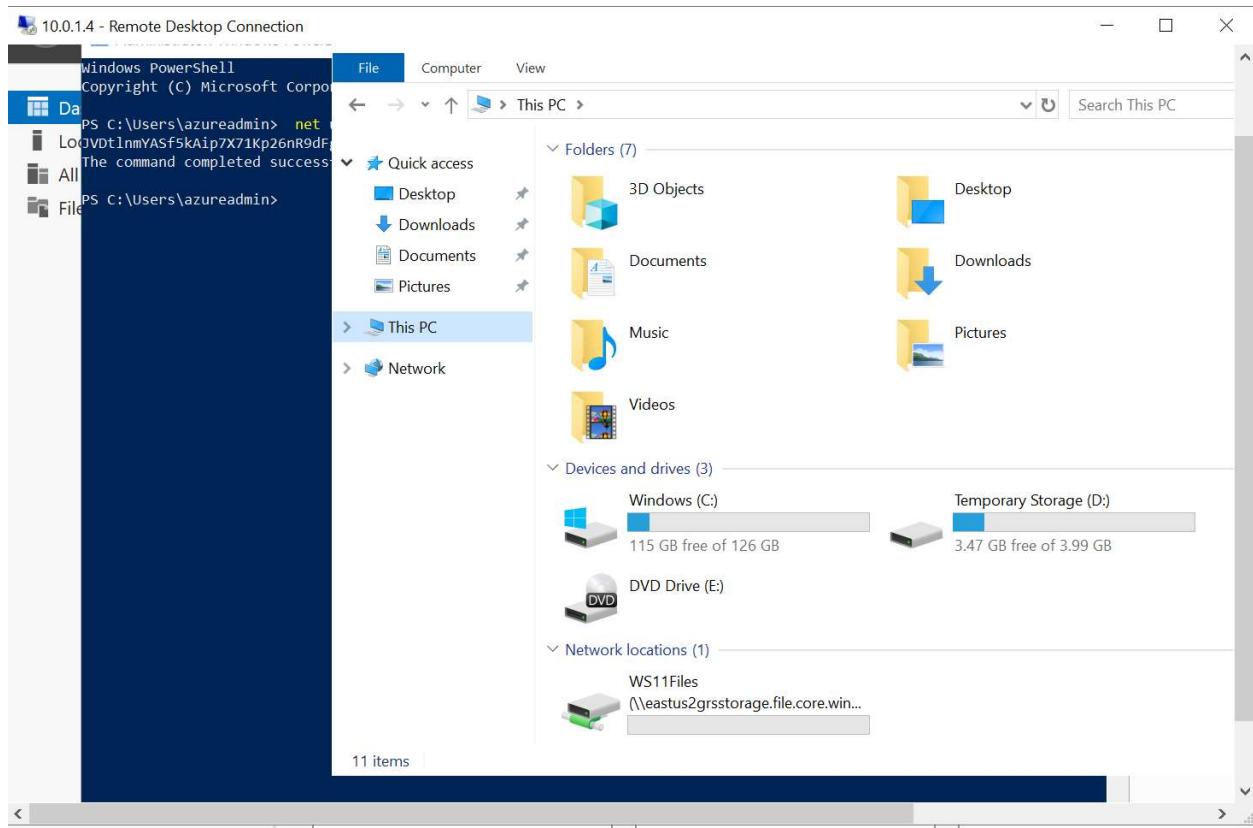
## 3. Map S: Drive on WS11

- **RDP to RDGateway** → connect to **WS11**.
- Run **PowerShell** →

```
net use S: \\eastus2grsstorage.file.core.windows.net\WS11Files /u:Azure\eastus2grsstorage Ue7QAJVDt1nmYASf5kAip7X71Kp26nR9dFgr6qBokJg3mv3Rkc0VzdnYfw9hKf8V DzD3aSh2lPm7+ASTCY41HQ==
```

The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The command entered is 'net use S: \\eastus2grsstorage.file.core.windows.net\WS11Files /u:Azure\eastus2grsstorage Ue7QAJVDt1nmYASf5kAip7X71Kp26nR9dFgr6qBokJg3mv3Rkc0VzdnYfw9hKf8V DzD3aSh2lPm7+ASTCY41HQ=='. The output shows the command completed successfully. The background of the window shows a taskbar with icons for File Explorer, Task View, Start, Task Manager, and others. The system tray indicates the date as 10/14/2025 and the time as 11:26 PM.

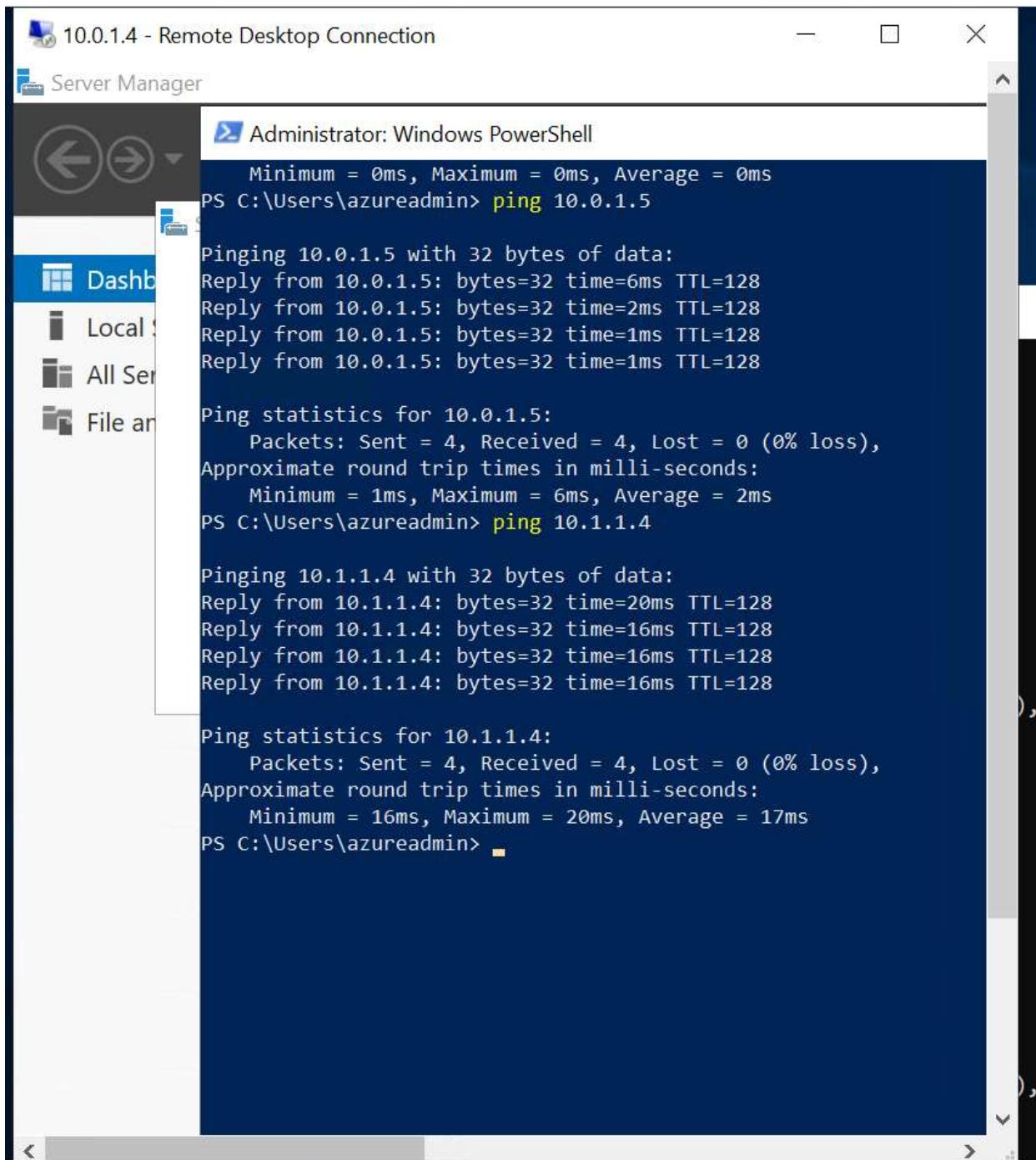
- Verify in File Explorer → **S: drive.**



#### 4. Connectivity Tests

- Ping between w1, w2, and WS11.

From W1 →



The screenshot shows a Windows Server Remote Desktop Connection window titled "10.0.1.4 - Remote Desktop Connection". Inside, a PowerShell window titled "Administrator: Windows PowerShell" is open. The user has run several "ping" commands:

- First, they pinged "10.0.1.5":

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\azureadadmin> ping 10.0.1.5
```

Pinging 10.0.1.5 with 32 bytes of data:  
Reply from 10.0.1.5: bytes=32 time=6ms TTL=128  
Reply from 10.0.1.5: bytes=32 time=2ms TTL=128  
Reply from 10.0.1.5: bytes=32 time=1ms TTL=128  
Reply from 10.0.1.5: bytes=32 time=1ms TTL=128

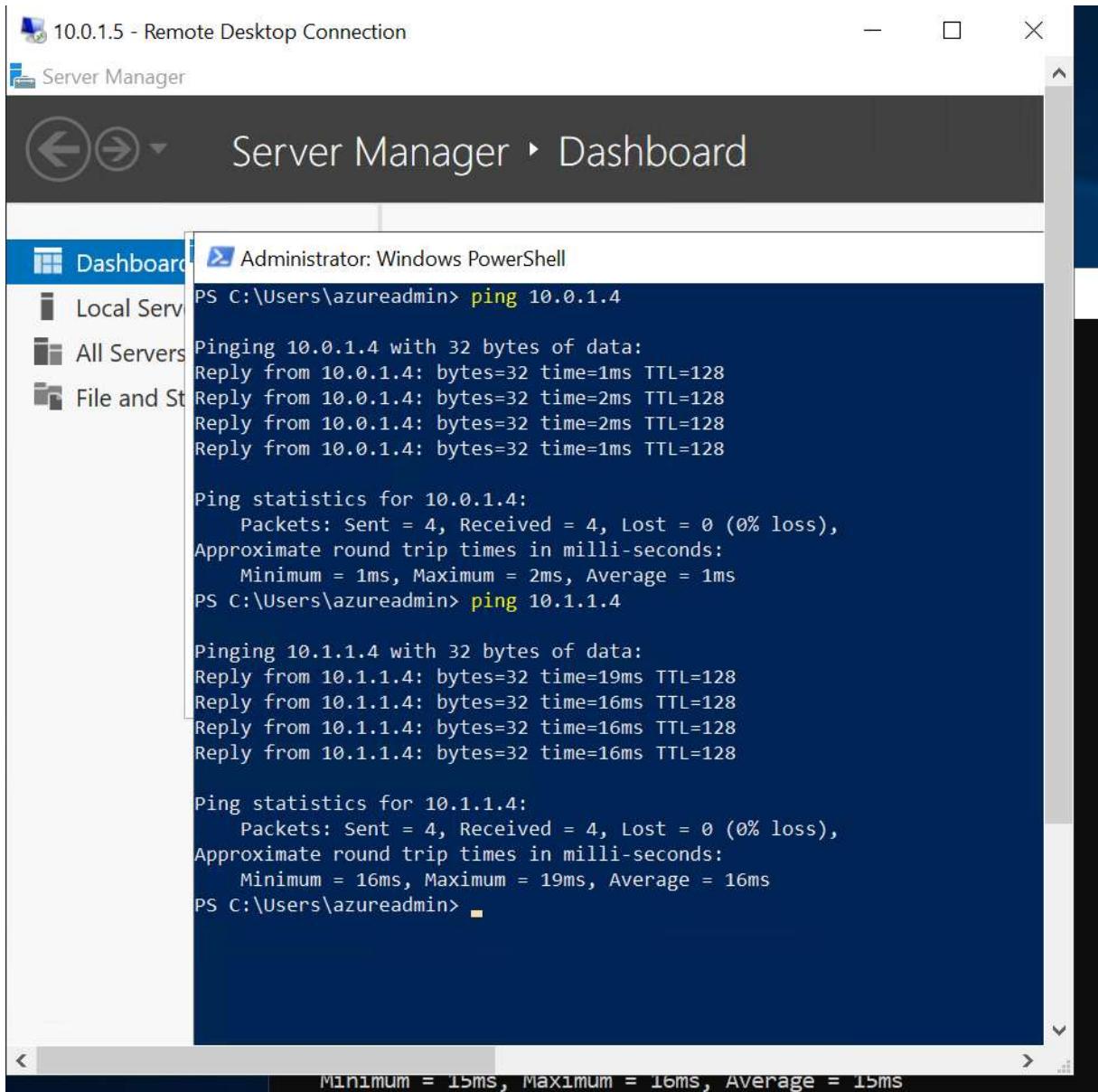
Ping statistics for 10.0.1.5:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 6ms, Average = 2ms
- Then, they pinged "10.1.1.4":

```
PS C:\Users\azureadadmin> ping 10.1.1.4
```

Pinging 10.1.1.4 with 32 bytes of data:  
Reply from 10.1.1.4: bytes=32 time=20ms TTL=128  
Reply from 10.1.1.4: bytes=32 time=16ms TTL=128  
Reply from 10.1.1.4: bytes=32 time=16ms TTL=128  
Reply from 10.1.1.4: bytes=32 time=16ms TTL=128

Ping statistics for 10.1.1.4:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 16ms, Maximum = 20ms, Average = 17ms

From W2 →



10.0.1.5 - Remote Desktop Connection

Server Manager

Administrator: Windows PowerShell

```
PS C:\Users\azureadmin> ping 10.0.1.4

Pinging 10.0.1.4 with 32 bytes of data:
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128

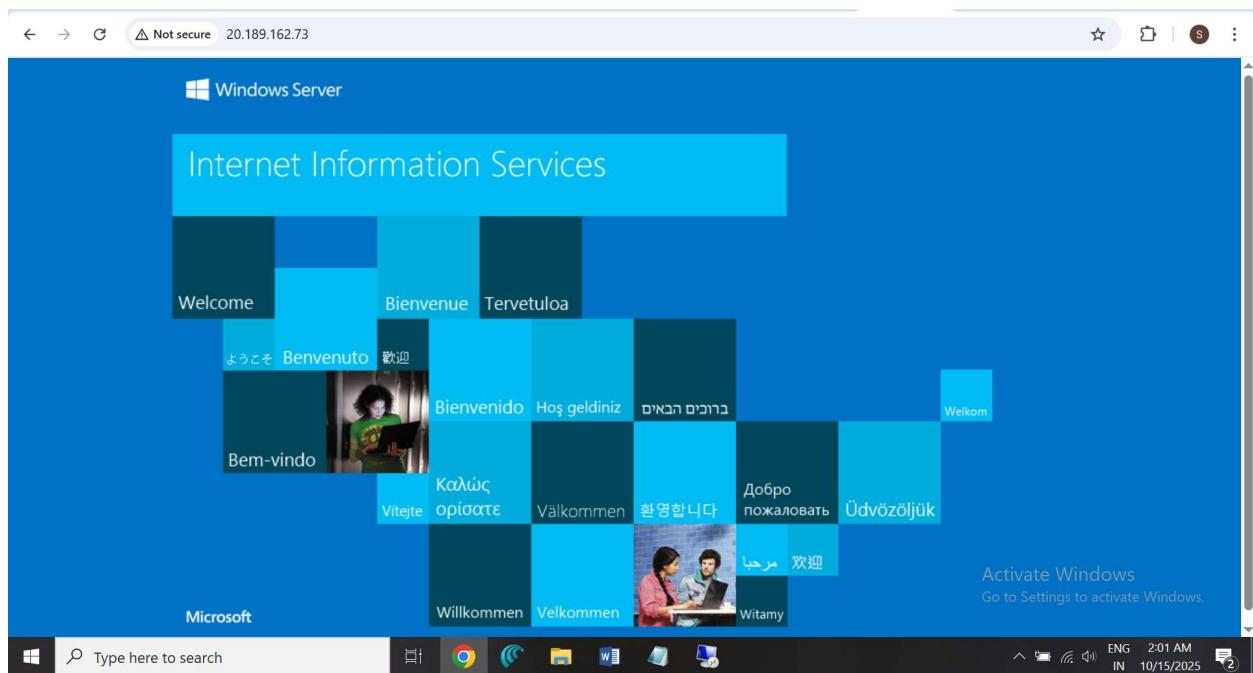
Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\azureadmin> ping 10.1.1.4

Pinging 10.1.1.4 with 32 bytes of data:
Reply from 10.1.1.4: bytes=32 time=19ms TTL=128
Reply from 10.1.1.4: bytes=32 time=16ms TTL=128
Reply from 10.1.1.4: bytes=32 time=16ms TTL=128
Reply from 10.1.1.4: bytes=32 time=16ms TTL=128

Ping statistics for 10.1.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 19ms, Average = 16ms
PS C:\Users\azureadmin>
```

MINIMUM = 15ms, Maximum = 16ms, Average = 15ms

- Access Load Balancer HTTP from browser.



## □ Verification

**Web page accessible**

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Home, Dashboard, All services, and Favorites. Under Favorites, there are links to Resource Manager, Resource groups, App Services, Function App, Azure SQL Database, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Microsoft Entra ID, Monitor, Advisor, Microsoft Defender for Cloud, Cost Management + Billing, and Create a resource.

The main content area displays the 'Compute infrastructure | Virtual machines' page. It shows a list of virtual machines: RDGateway, w1, w2, and WS11. The RDGateway VM is selected. To the right, a detailed view of the RDGateway VM is shown, including its Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking (with Network settings), Settings, Disks, and Extensions + automation.

A modal window titled 'Add inbound security rule' is open on the right. It is configured to allow inbound HTTPS (RDP) over TCP port 443. The settings include:

- Destination:** Any
- Service:** Custom
- Destination port ranges:** 443
- Protocol:** TCP (selected)
- Action:** Allow (selected)
- Priority:** 101
- Name:** Allow-HTTPS-RDGateway
- Description:** Allow inbound HTTPS (RDP) over TCP port 443

## ❖ Visual Diagram:

- Project Architecture Diagram→

