Assignment -9

Hyper V

Stablish S2S Connection hyper-v (child VM) Vm to azure

Ananya Srivastava
CLOUD INFRA

Table of Contents

1. Introduction

A Site-to-Site (S2S) Virtual Private Network (VPN) connection allows secure communication between two networks over the internet. In this document, we will guide you through the process of establishing an S2S connection between a Hyper-V child VM and Microsoft Azure. This setup is particularly useful for extending your on-premises network to Azure, ensuring seamless connectivity and data transfer between your local environment and Azure resources.

2. Prerequisites

Before starting, ensure you have the following:

- A Hyper-V host with a child VM running Windows Server.
- An active Azure subscription.
- Basic understanding of networking concepts.
- Administrator access to both the Hyper-V child VM and the Azure portal.

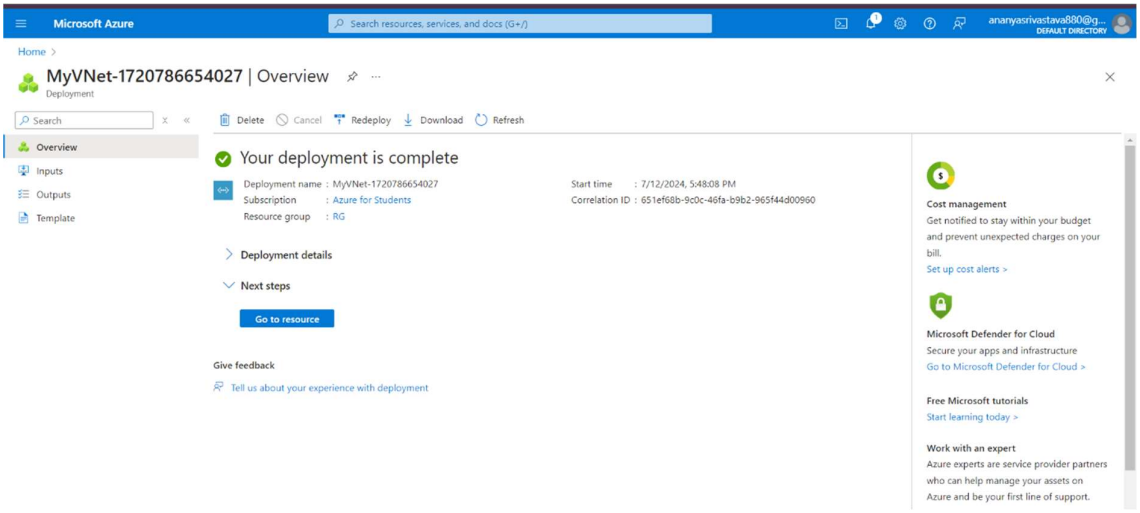
3. Setting Up the Hyper-V Environment

1. **Install Hyper-V Role**: Ensure Hyper-V is installed on your host machine.
2. **Create a Virtual Machine**: Set up a Windows Server VM that will act as the local network endpoint.
3. **Configure Networking**: Assign a static IP to the VM and ensure it has internet access.

4. Steps to Establish Site-to-Site VPN Connection from Hyper-V (Child VM) to Azure

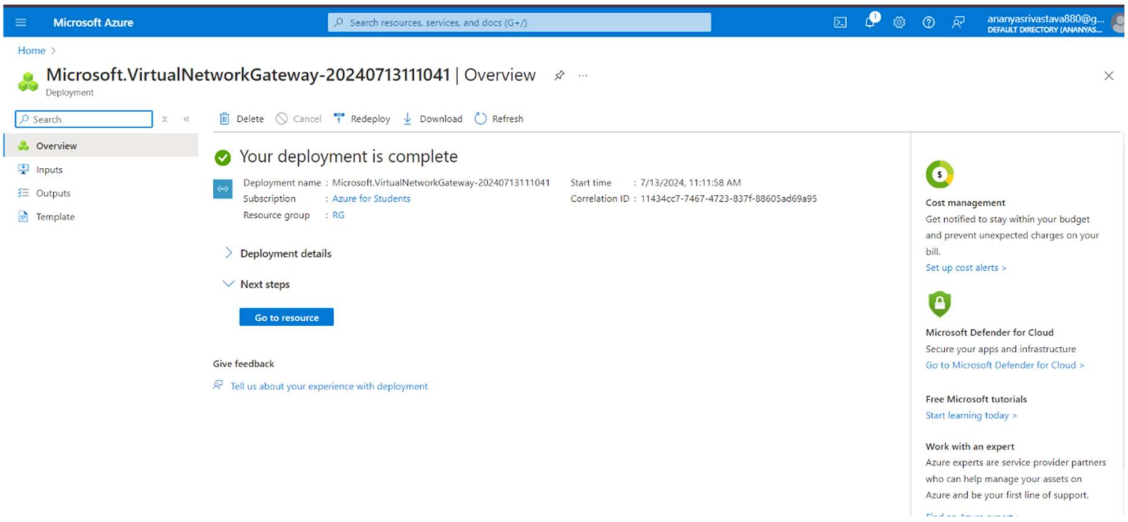
Step 1: Create a Virtual Network in Azure

1. **Navigate to the Azure Portal**.
2. **Create a Virtual Network**:
    - Go to Create a resource > Networking > Virtual network.
    - Enter the details such as Name, Address space, Subnet name, and Subnet address range.
    - Click Review + create and then Create.



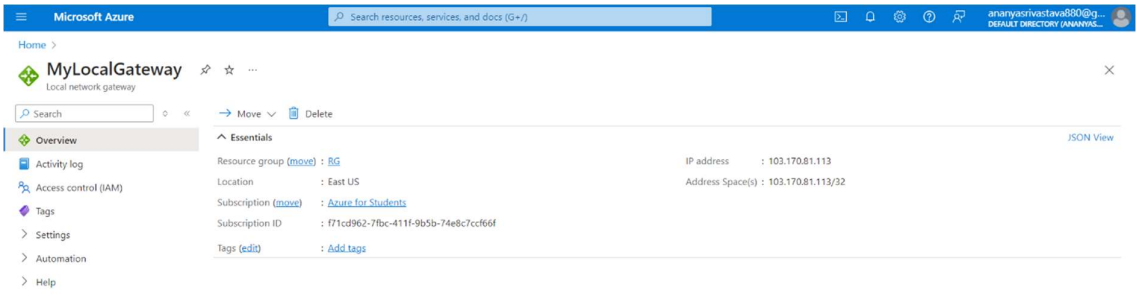
Step 2: Create a Virtual Network Gateway

1. **Navigate to the Azure Portal**.
2. **Create a Virtual Network Gateway**:
    - Go to Create a resource > Networking > Virtual network gateway.
    - Enter the details:
        - Name: MyGateway
        - Region: Select the same region as your virtual network.
        - Gateway type: VPN
        - VPN type: Route-based
        - SKU: Select the SKU based on your requirement (e.g., VpnGw1).
        - Virtual network: Select the virtual network you created.
        - Public IP address: Create a new one.
    - Click Review + create and then Create.



Step 3: Create a Local Network Gateway

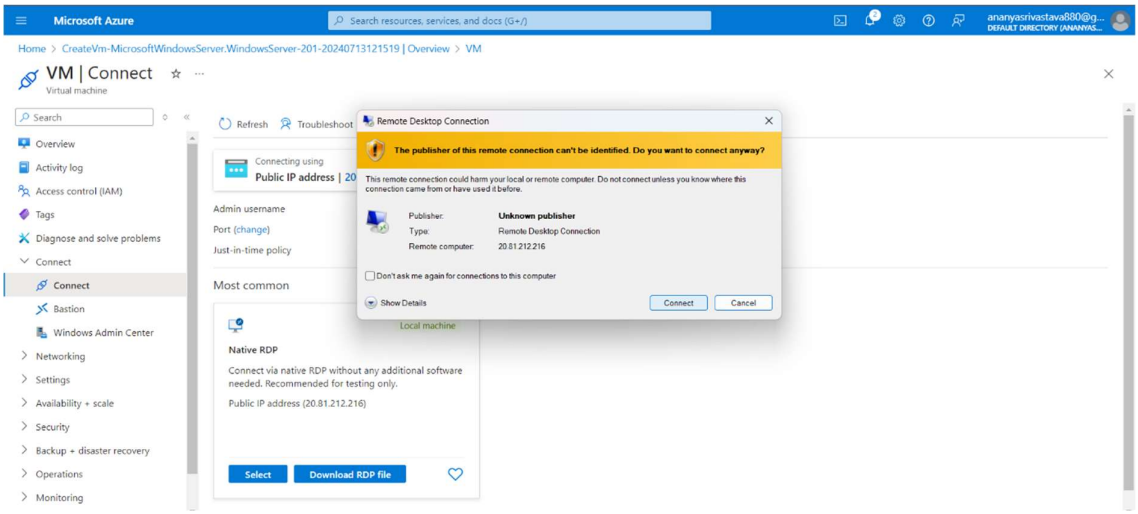
1. **Navigate to the Azure Portal**.
2. **Create a Local Network Gateway**:
    - Go to Create a resource > Networking > Local network gateway.
    - Enter the details:
        - Name: MyLocalGateway
        - IP address: Enter your on-premises public IP address.
        - Address space: Enter the address space of your on-premises network (e.g., 10.1.0.0/16).
    - Click Review + create and then Create.

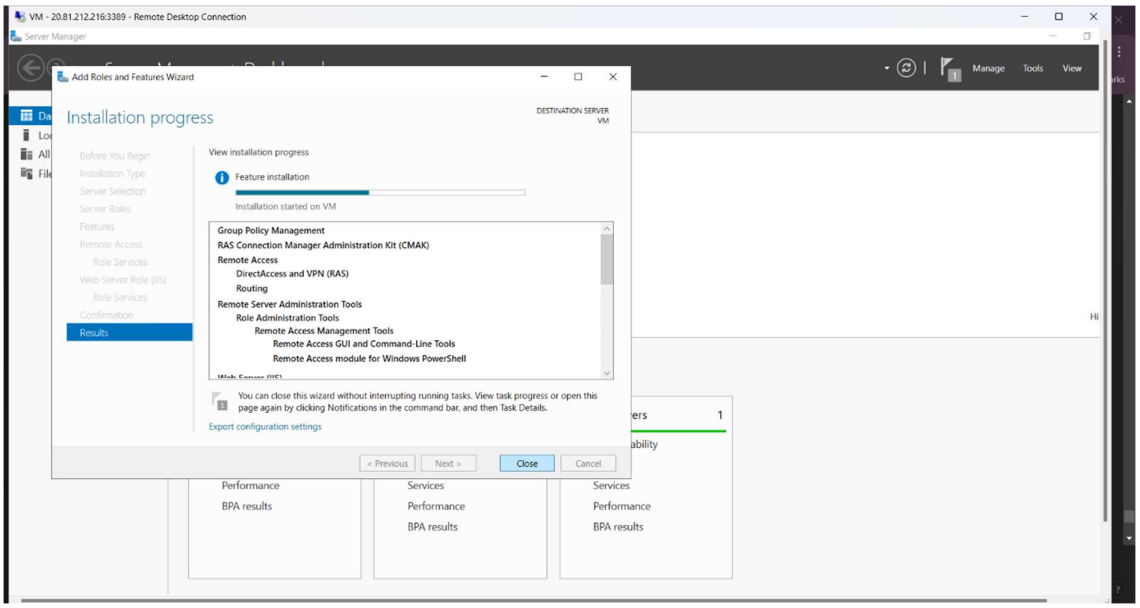


Step 4: Configure the VPN Gateway on Hyper-V

1. **Set up RRAS (Routing and Remote Access Service) on Hyper-V**:
    - Open Server Manager on the Hyper-V host.

- Add the Remote Access role and select Routing.

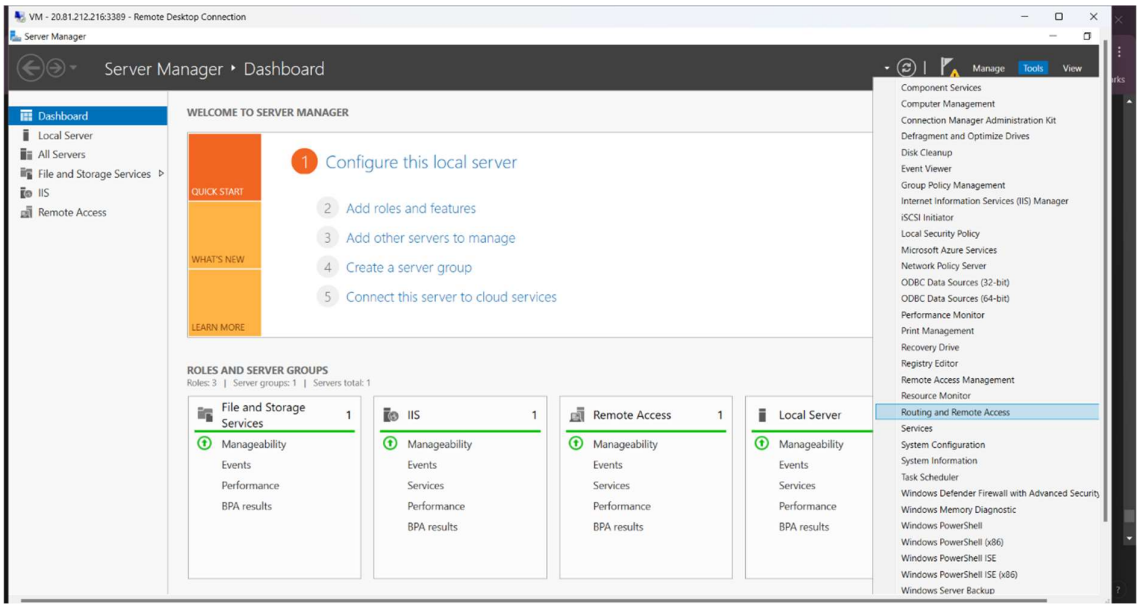


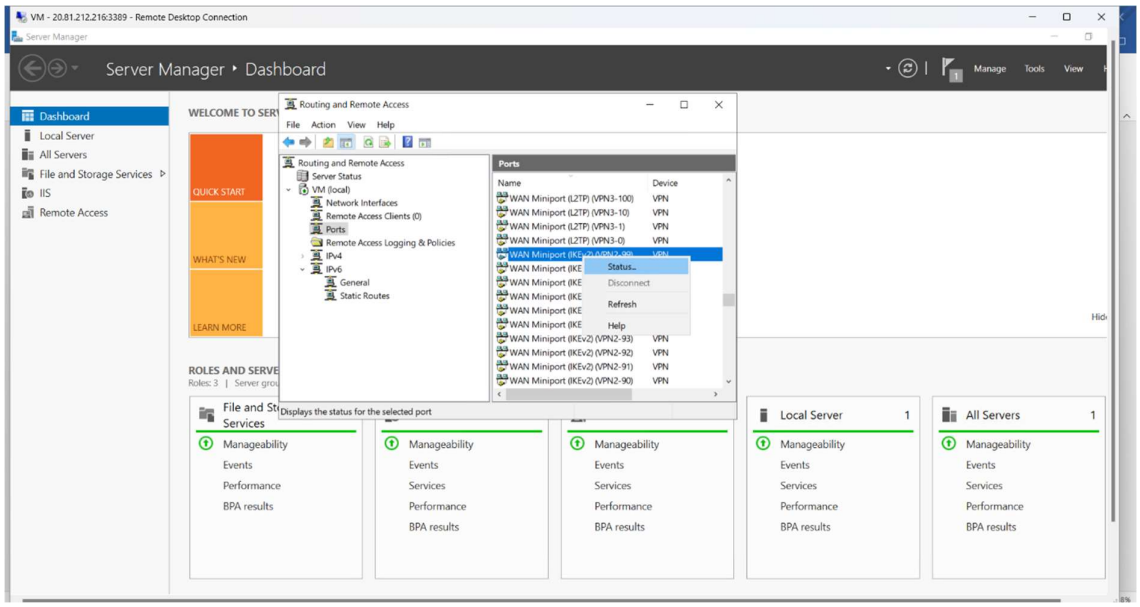


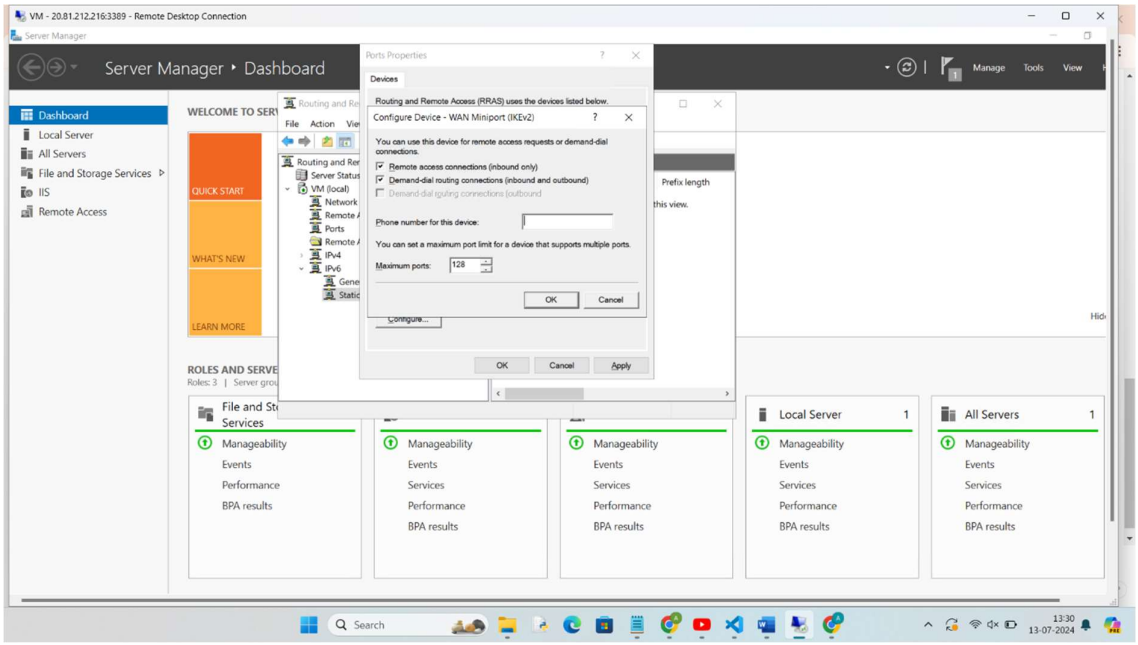
- Configure and enable Routing and Remote Access.
- Set up as Custom configuration and select VPN Access.

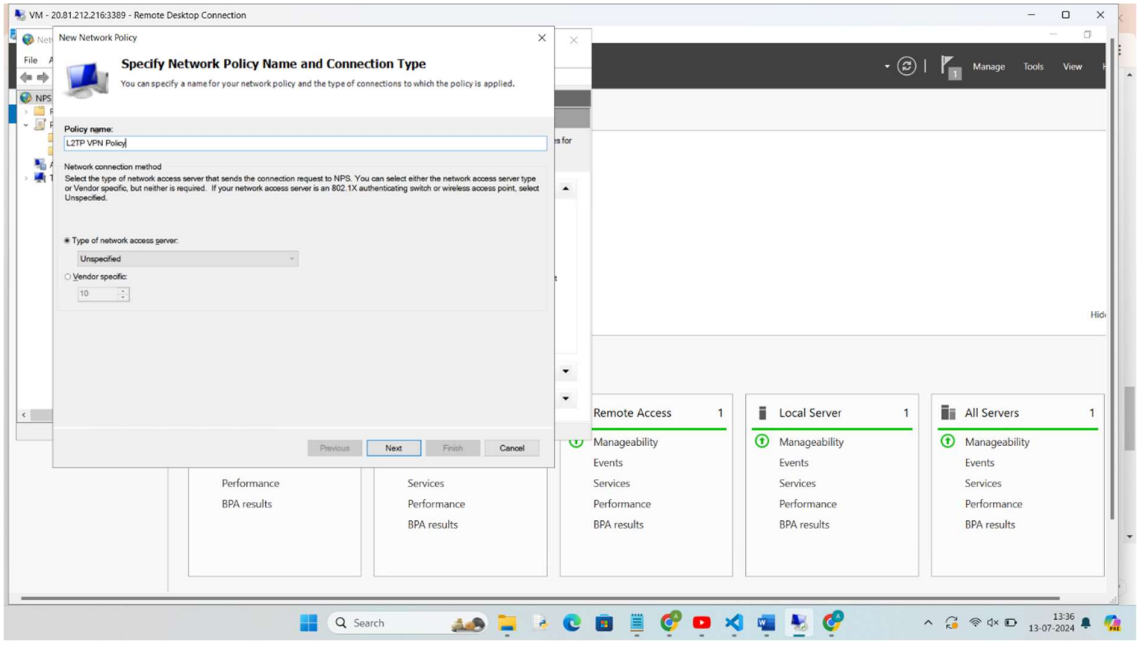
2. **Configure RRAS**:

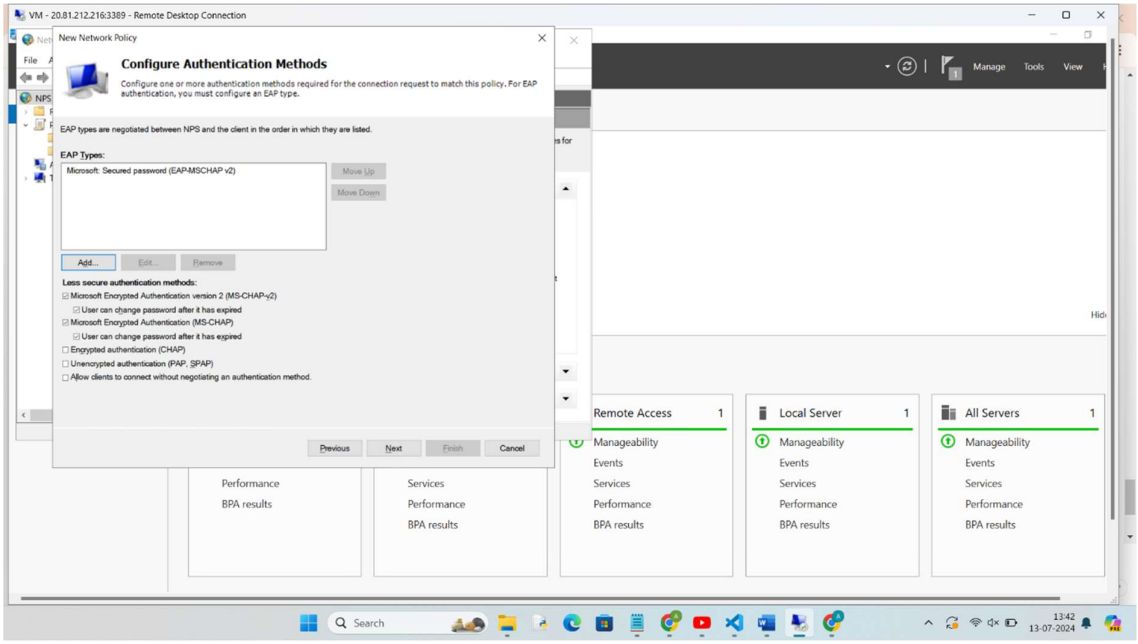
- Right-click on the server and select Configure and Enable Routing and Remote Access.
- Choose Custom configuration and select VPN access and NAT.
- Configure VPN to use L2TP/IPsec and set up shared secret.





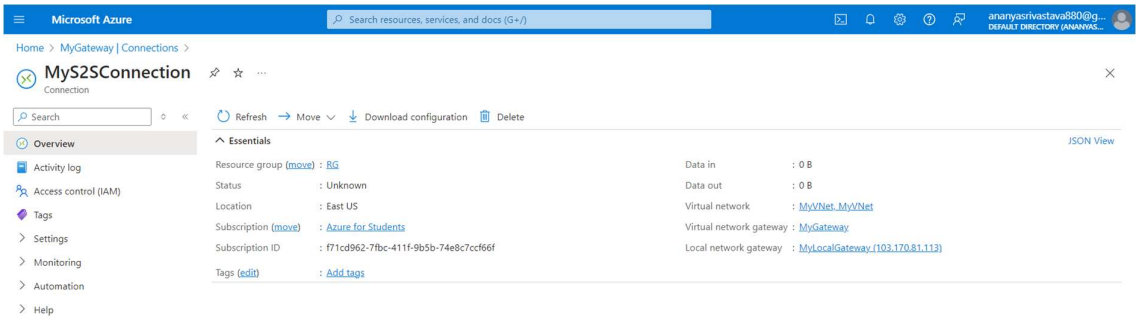

VM - 20.81.212.216:3389 - Remote Desktop Connection
Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Remote Access
WELCOME TO SERV
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVE
Roles: 3 | Server grou
Ports Properties
Devices
Routing and Remote Access (RRAS) uses the devices listed below.
Configure Device - WAN Miniport (IKEv2)
You can use this device for remote access requests or demand-dial connections.
Remote access connections (inbound only)
Demand-dial routing connections (inbound and outbound)
Demand-dial routing connections (outbound
Phone number for this device:
You can set a maximum port limit for a device that supports multiple ports.
Maximum ports:
128
OK
Cancel
Apply
Routing and Re
File Action Vie
Server Status
VM (local)
Network
Ports
IPv4
IPv6
Prefix length
this view.
File and St
Services
Manageability
Events
Performance
BPA results
Services
Local Server
1
All Servers
1
Search
13:30
13-07-2024


VM - 20.81.212.216:3389 - Remote Desktop Connection
New Network Policy
Specify Network Policy Name and Connection Type
You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name:
L2TP VPN Policy
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10
Previous
Next
Finish
Cancel
Manage
Tools
View
Remote Access 1
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results
All Servers 1
Manageability
Events
Services
Performance
BPA results
Search
13:36
13-07-2024

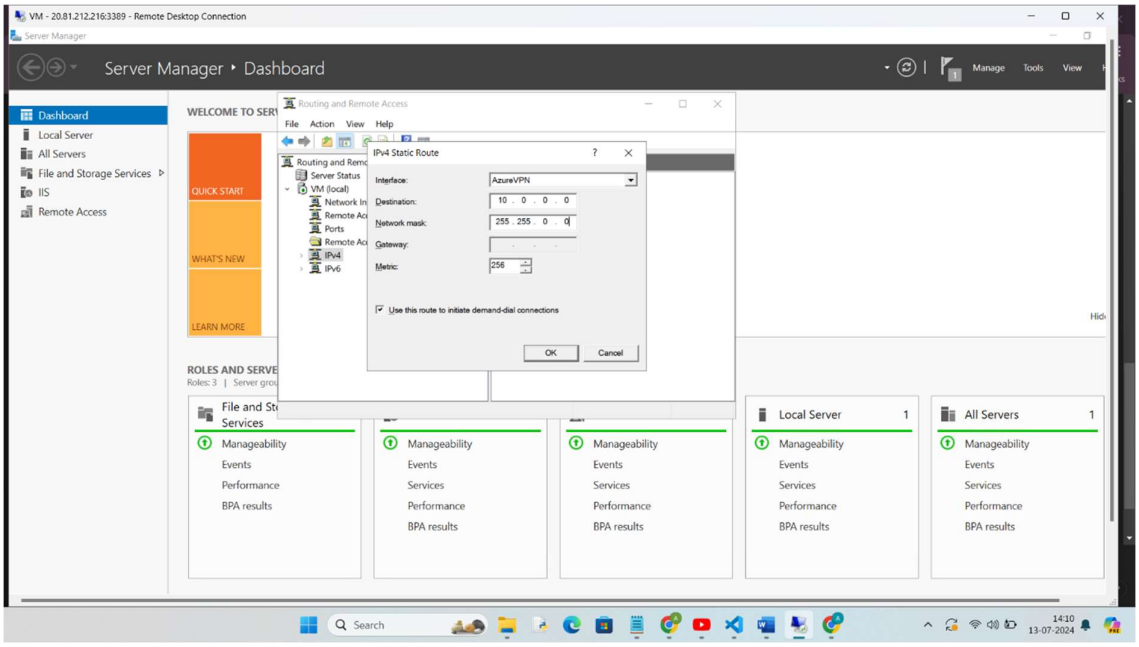

VM - 20.81.212.216:3389 - Remote Desktop Connection
New Network Policy
Configure Authentication Methods
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.
Previous
Next
Finish
Cancel
Manage
Tools
View
Remote Access 1
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results
All Servers 1
Manageability
Events
Services
Performance
BPA results
Search
13:42
13-07-2024

Step 5: Create a VPN Connection

1. **On Azure Portal**:
   - Go to Virtual network gateway > Connections > Add.
   - Enter the details:
     - Name: MyS2SConnection
     - Connection type: Site-to-site (IPsec)
     - Virtual network gateway: Select your virtual network gateway.
     - Local network gateway: Select your local network gateway.
     - Shared key: Enter the same shared secret used in RRAS configuration.
   - Click OK to create the connection.

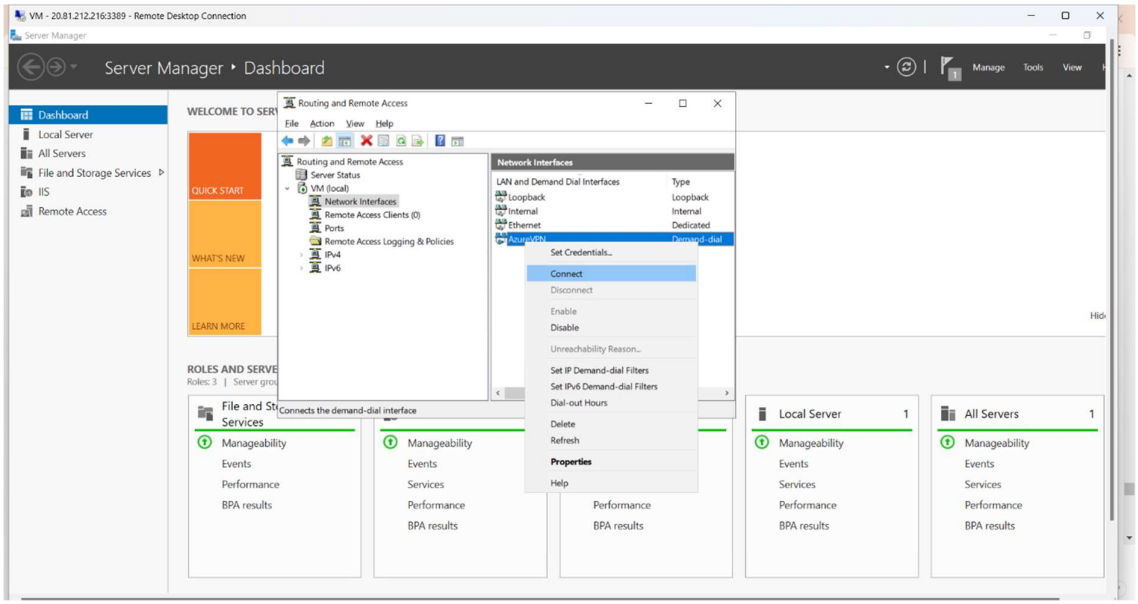


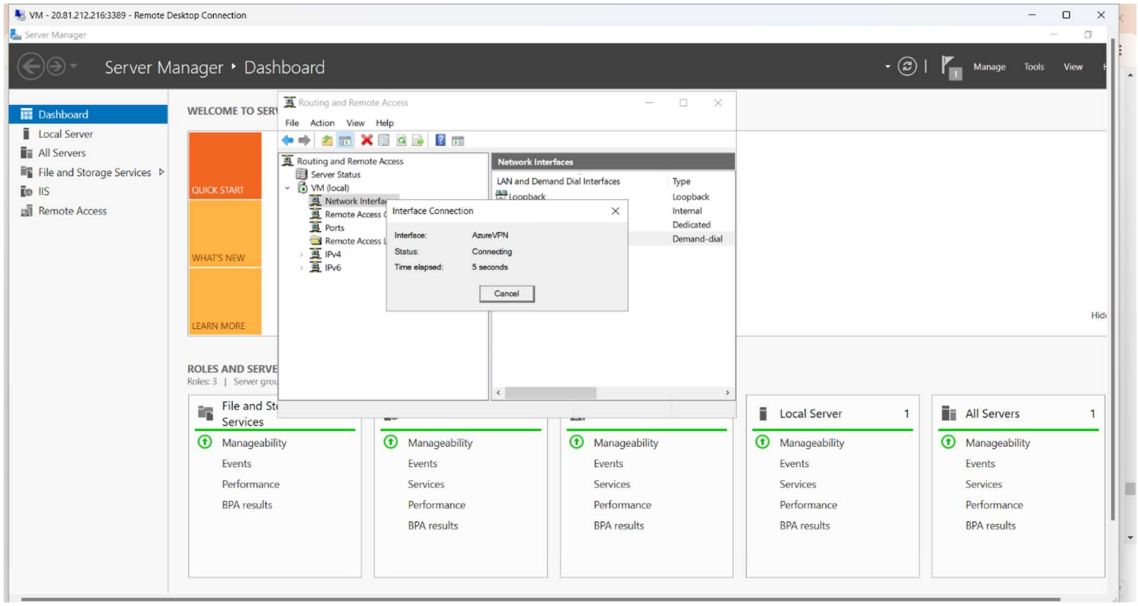
2. **On Hyper-V**:
   - Open Routing and Remote Access console.
   - Right-click on Network Interfaces and add a new Demand-dial interface.
   - Configure the interface to use VPN and enter the Azure gateway public IP.
   - Set up IPsec with the same shared secret used in Azure.

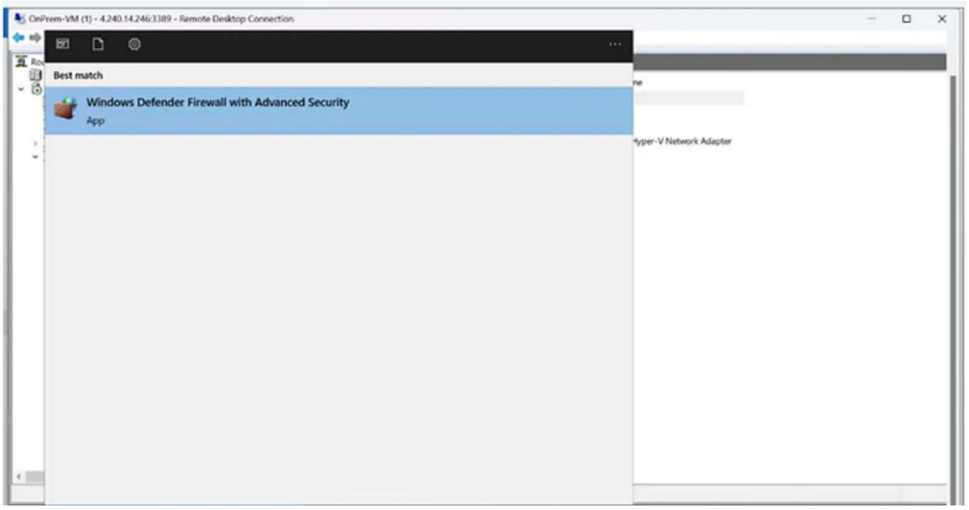


Step 6: Verify the Connection

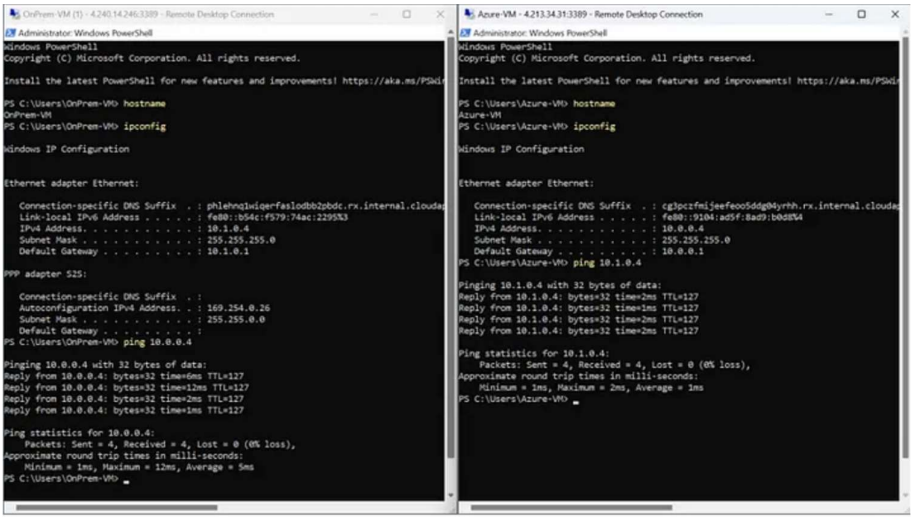
1. **Check Connection Status**:
   - In Azure Portal, navigate to Virtual network gateway > Connections.
   - Verify the connection status is Connected.







2. **Test Connectivity**:
    - From a VM in your on-premises network, try to ping a VM in the Azure virtual network.



5. Troubleshooting

1. **Check IP Configurations**: Ensure all IP addresses and subnets are correctly configured.
2. **Verify Shared Key**: The shared key must match on both ends.
3. **Firewall Rules**: Ensure necessary ports (e.g., UDP 500, 4500) are open.
4. **Logs and Diagnostics**: Use Azure's diagnostic tools and RRAS logs to identify issues.

6. Conclusion

Establishing an S2S VPN connection between a Hyper-V child VM and Azure extends your local network to the cloud, enabling secure and reliable communication. This document provides a step-by-step guide to achieve this setup, ensuring your hybrid cloud environment is effectively integrated.

7. References

1. Microsoft Documentation: Site-to-Site VPN - https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

2. Hyper-V Networking Guide- https://learn.microsoft.com/en-us/windows-server/networking/sdn/technologies/hyper-v-network-virtualization/hyperv-network-virtualization-overview-windows-server

3. Azure VPN Gateway Documentation-https://learn.microsoft.com/en-us/azure/vpn-gateway/

4. Routing and Remote Access Service (RRAS) Overview-https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/set-up-routing-remote-access-intranet