😊 Azure Virtual WAN

Azure Virtual WAN is a networking service provided by Microsoft Azure that allows you to connect and manage multiple branch offices, data centers, and remote users securely through the Microsoft global network. It simplifies connectivity by providing a unified hub for connecting various network environments.

Key features of Azure Virtual WAN include:

1. **Hub and Spoke Architecture:** Virtual WAN employs a hub and spoke model, where the hub serves as a central point of connectivity for branches, remote users, and Azure Virtual Networks (VNets).
2. **Global Reach:** It leverages Microsoft's global network infrastructure to provide low-latency and high-performance connectivity across regions.
3. **Secure Connectivity:** Virtual WAN offers built-in encryption, authentication, and security features to ensure secure communication between network resources.
4. **Integration with Azure Services:** It seamlessly integrates with other Azure networking services such as Azure VPN Gateway, Azure Firewall, and Azure ExpressRoute.
5. **Centralized Management:** Administrators can manage and monitor the entire network infrastructure from a central Azure portal, simplifying deployment and troubleshooting.
6. **Optimized Routing:** Virtual WAN dynamically routes traffic based on performance metrics, ensuring optimal connectivity and minimal latency.
7. **Third-party Integration:** It supports integration with third-party networking appliances and services through Virtual WAN partners.

Overall, Azure Virtual WAN streamlines network connectivity and management for organizations with distributed infrastructures, offering scalability, security, and performance.

😄 Use cases of Virtaul Azure WAN:

Azure Virtual WAN can be beneficial for various use cases, including:

1. **Branch Office Connectivity:** Organizations with multiple branch offices can use Virtual WAN to connect them securely to their headquarters or central data centers. This facilitates efficient communication and access to corporate resources while maintaining network security.
2. **Global Network Expansion:** Companies expanding their operations globally can leverage Virtual WAN to establish connectivity between different regions. It provides a unified platform for managing network connectivity across geographically dispersed locations, ensuring consistent performance and security.
3. **Remote User Access:** With the rise of remote work, Virtual WAN can enable secure connectivity for remote users accessing corporate resources from

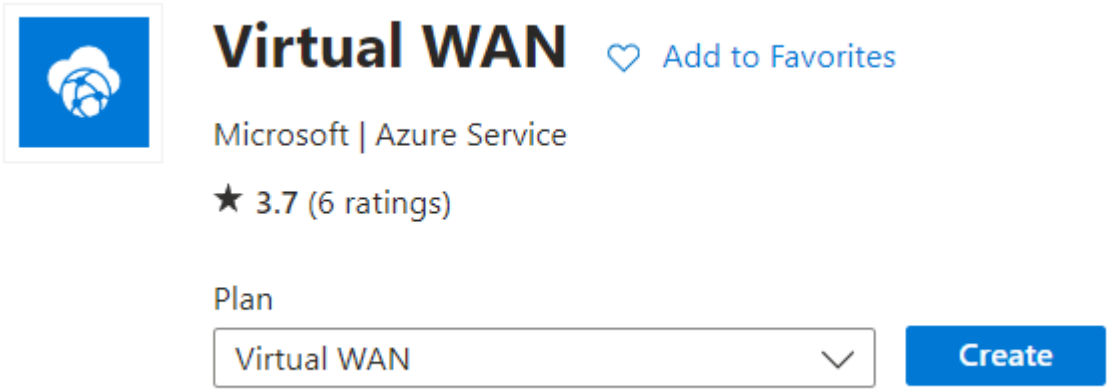
anywhere in the world. It provides a reliable and secure VPN solution for remote access, ensuring that employees can work effectively while maintaining data security.

4. **Hybrid Cloud Connectivity:** Organizations adopting a hybrid cloud approach can use Virtual WAN to connect their on-premises data centers to Azure and other cloud environments. This enables seamless communication between on-premises resources and cloud-based services, facilitating workload migration and hybrid IT deployments.
5. **Highly Available Network Architecture:** Virtual WAN supports redundant connections and automatic failover, ensuring high availability and reliability for critical network services. This is particularly beneficial for mission-critical applications that require uninterrupted connectivity.
6. **Optimized Internet Access:** By integrating with Azure Firewall and third-party security services, Virtual WAN can provide optimized internet access for branch offices and remote users. It enables organizations to enforce security policies and inspect internet-bound traffic without compromising performance.
7. **Centralized Network Management:** Virtual WAN offers centralized management and monitoring capabilities, allowing administrators to configure and monitor network connectivity from a single location. This simplifies network administration tasks and reduces the complexity of managing distributed network environments.

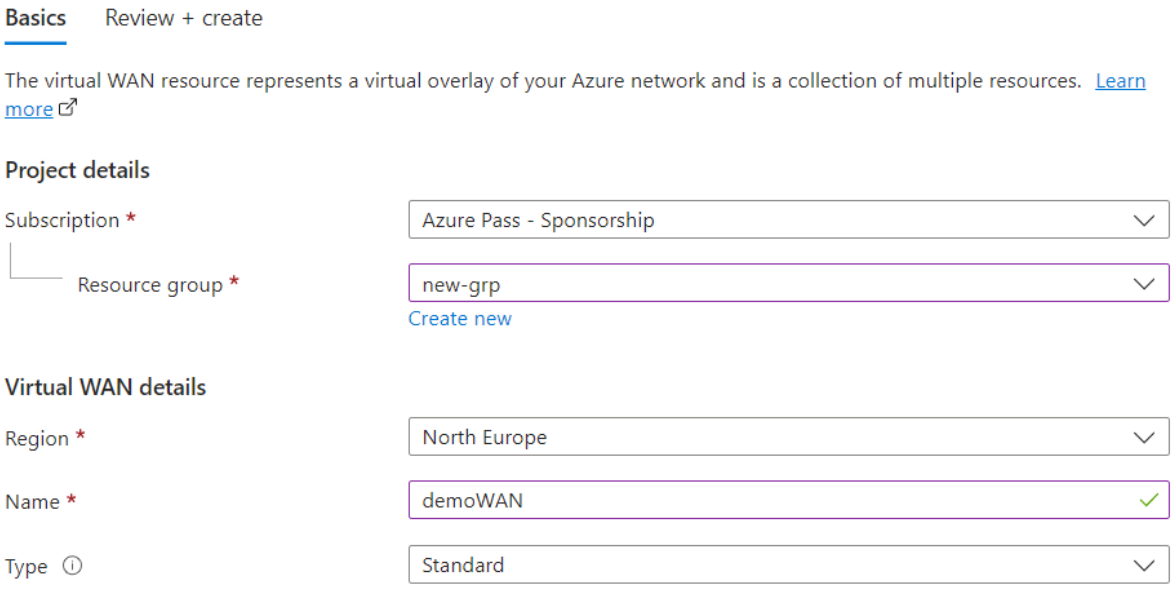
The end goal is to establish secure and efficient connectivity between the two VMs via Azure Virtual WAN and to enable remote access to these VMs through a User VPN. This setup demonstrates how to use Azure Virtual WAN for managing distributed network environments securely and efficiently.

😄 To begin with the Lab:

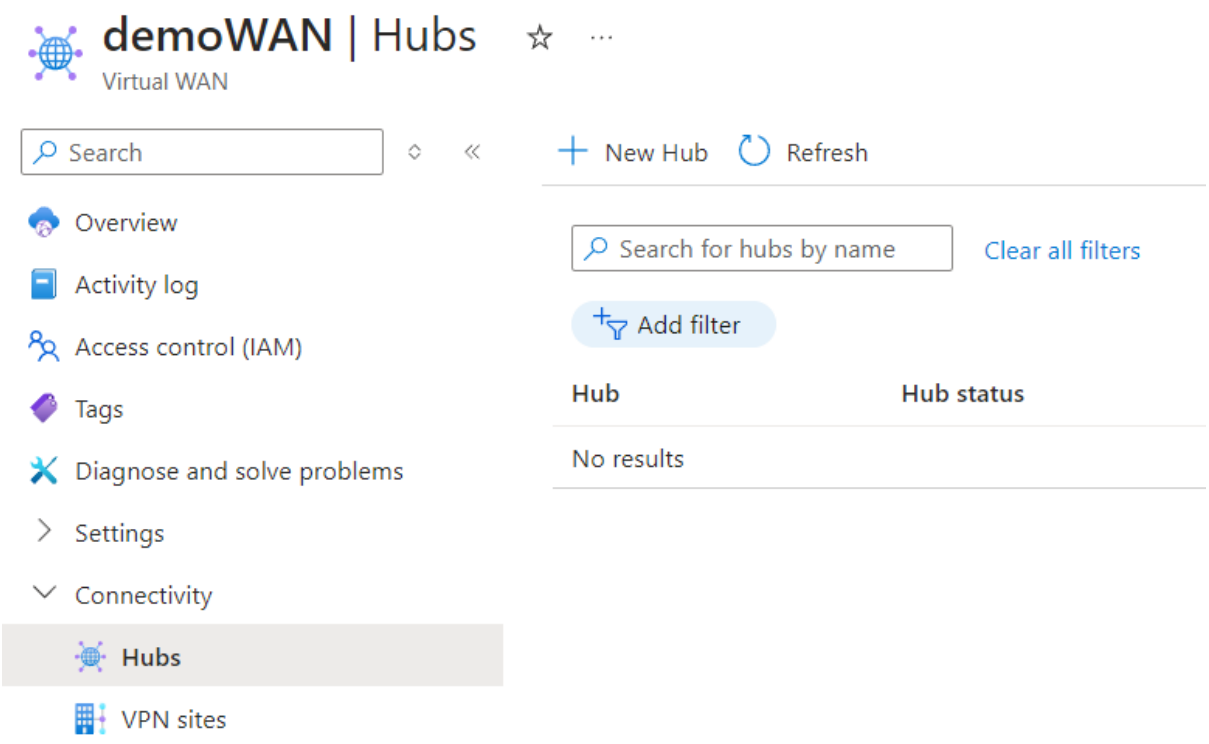
1. There are some prerequisites for this lab, you have to create two Virtual Machines based on Windows Server 2022. Also, you have to make sure that they get launched on different virtual networks with different address space.
2. After that you need to launch these virtual machines, install a Web Server (IIS) on them, and create a default HTML page to identify them like we did in our previous labs.
3. Once you are done with the setup then you need to disassociate the Public IP addresses from both of them and delete them from the resources.
4. After that you need to go to the marketplace and search for Virtual WAN and choose this service accordingly.



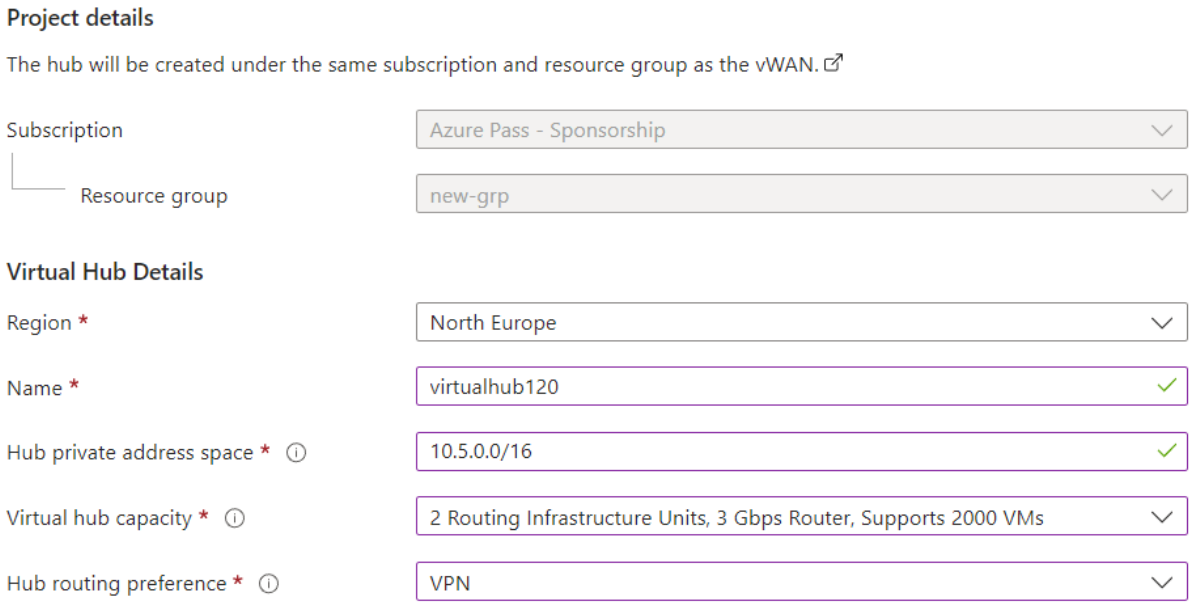
5. Then you need to choose your resource group and give it a name then choose type as Standard.



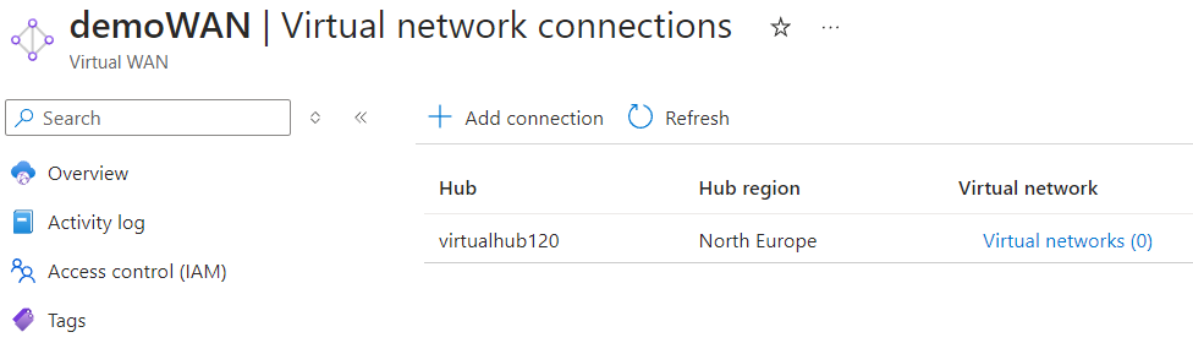
6. Once the deployment is completed then you need to go towards it and from the connectivity choose hubs and choose to create a new hub.



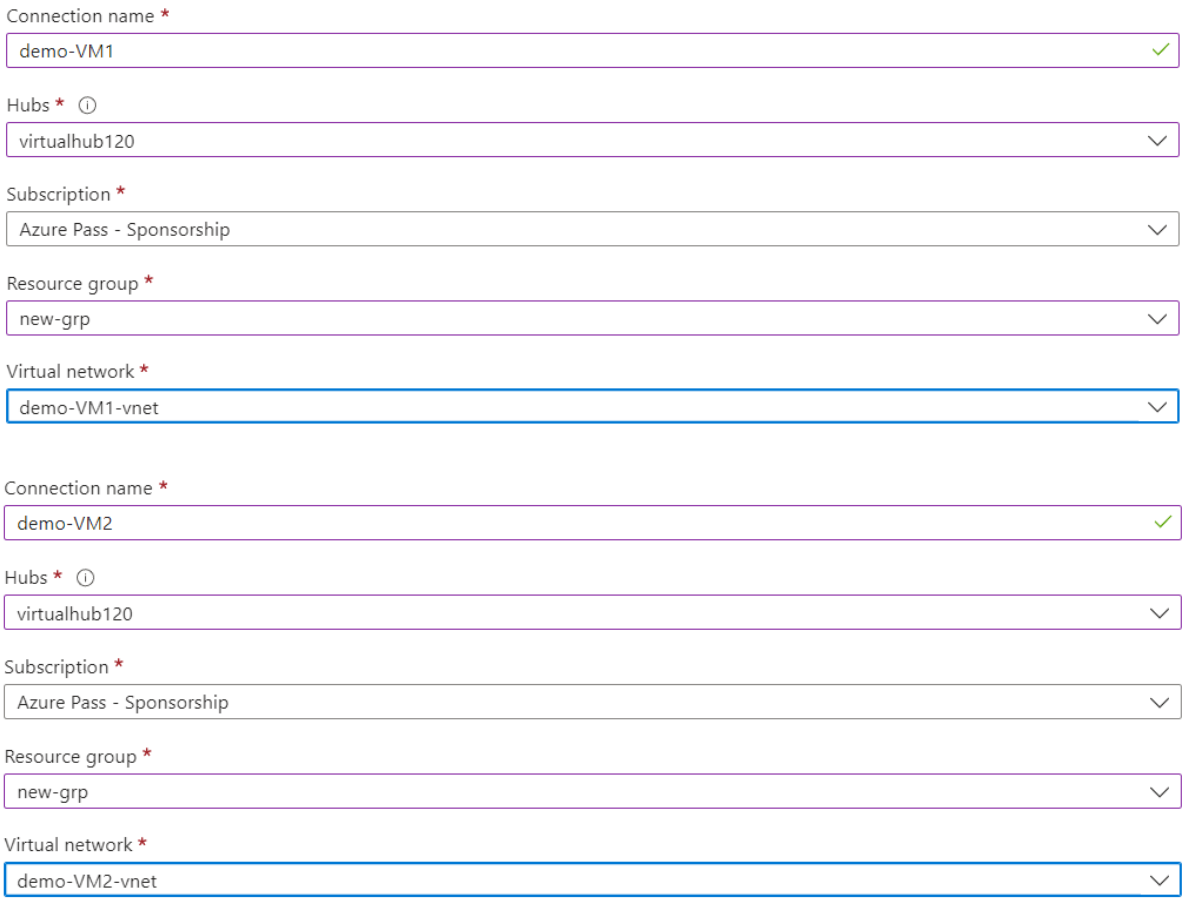
7. Now you need to choose your region, give it a unique name and then you need to give a private address space to it of your choice then for capacity and routing preference choose from the snapshot.



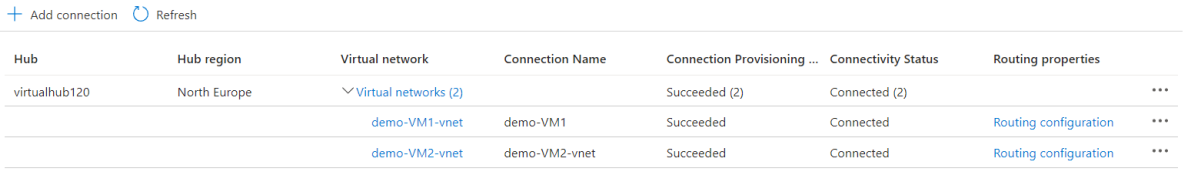
8. After that move to review page and choose to create your hub. Also, it will take almost 30 minutes for the hub to be in place.
9. Once the deployment is complete then come back to Virtual WAN and go to Virtual network connections and choose to add a connection.



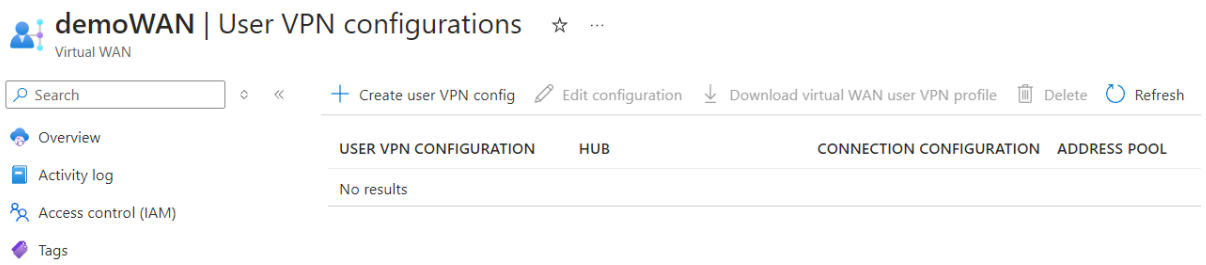
10. Now you need to give your connection a name that will be the same as your VM name, then choose your hub and the resource group then keep the rest settings to default. After that choose your virtual network. You need to do the same thing for other VMs too, choose to add a connection.



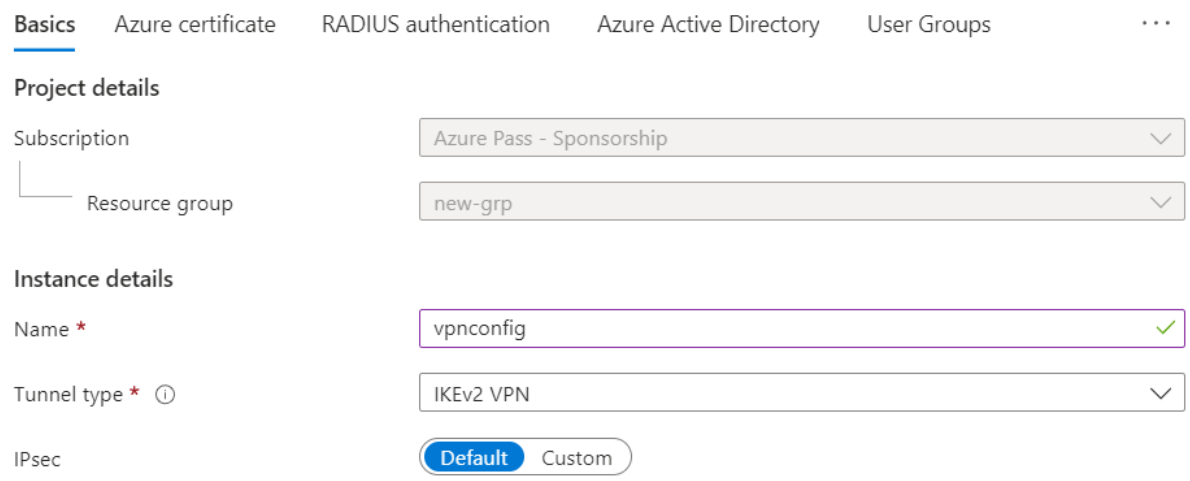
11. Below you can see that both of the connections are added.



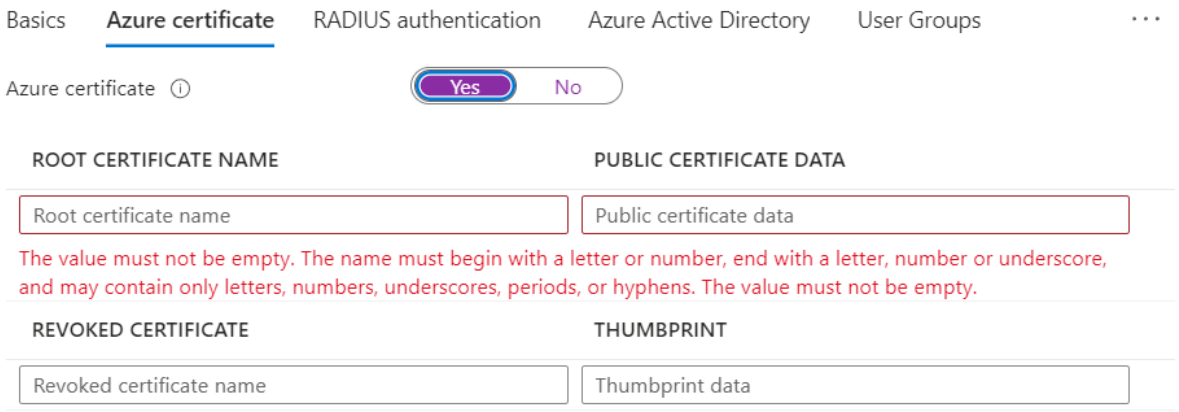
12. After that we need to go to the user VPN configuration and create one.

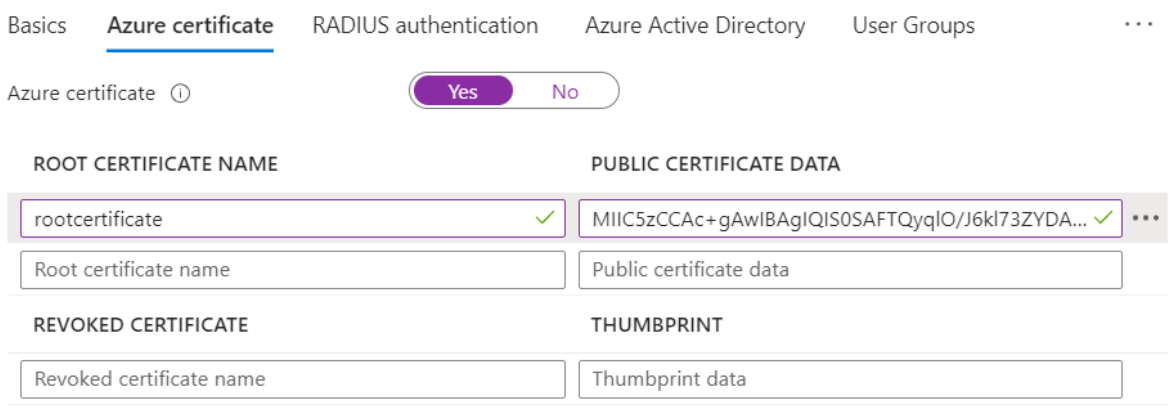


13. Then give it a name and then keep things to default.

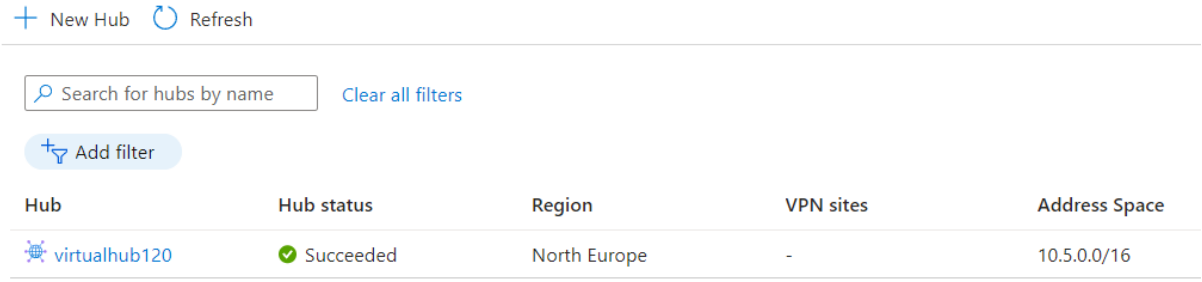


14. Here you can see that we need to add an Azure certificate and we can make use of the previous certificate that we used earlier.

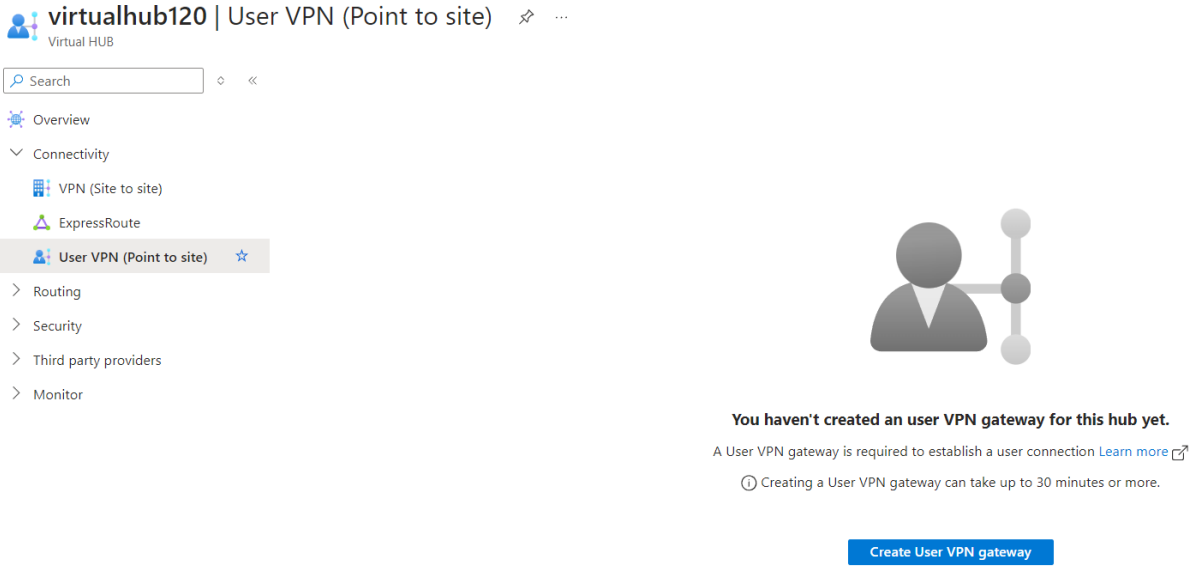




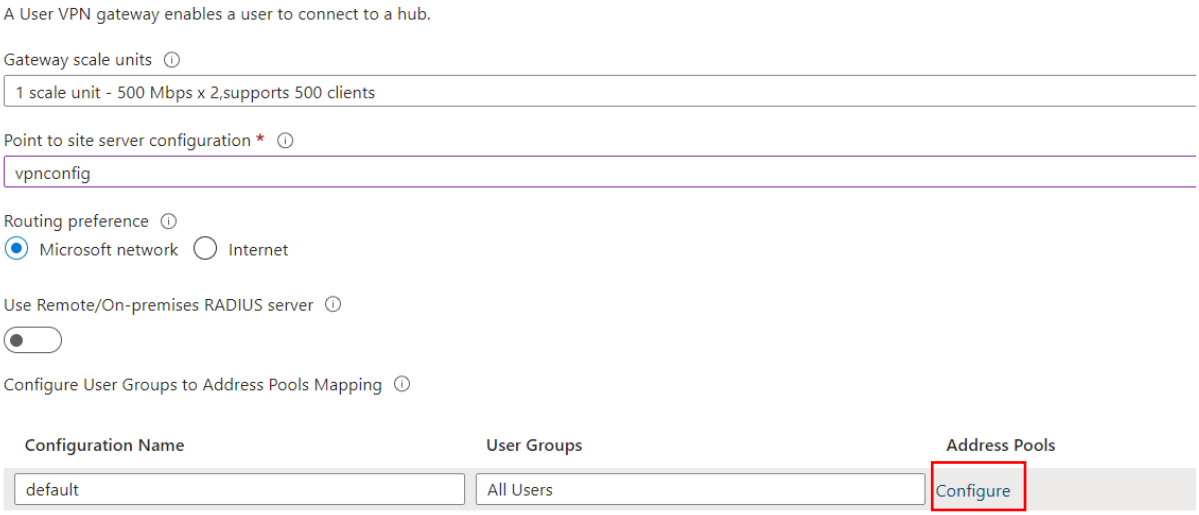
15. Now move to the review page and create your VPN config.
16. Then go to hubs and open it.



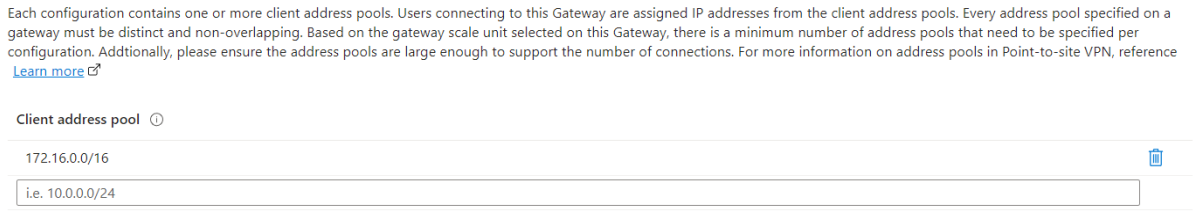
17. Then you need to go to User VPN (Point-to-Site) and create a User VPN gateway.



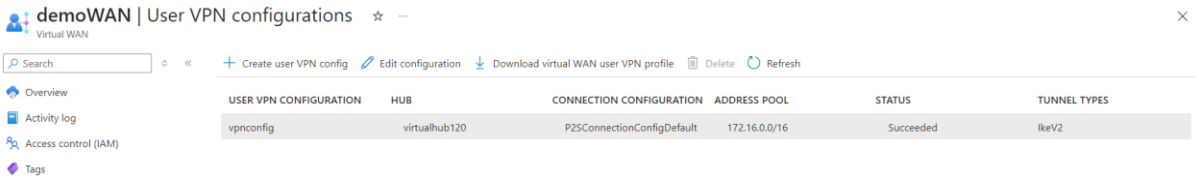
18. Now you need to choose gateway scale units choose the least unit. Then choose your point-to-site server configuration. After that keep routing preference to default. Then you need to click on configure for address pools.



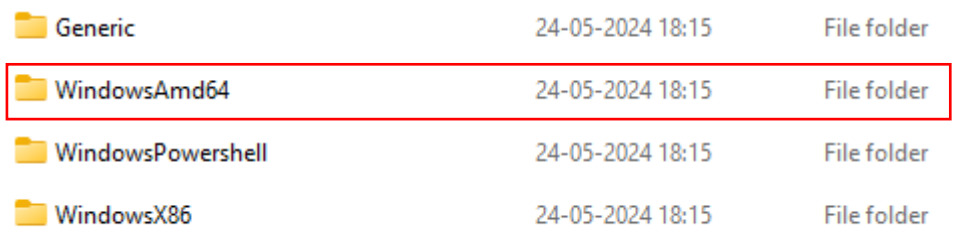
19. Then you have to specify the client address pool as shown below. You can use the same address pool.



20. Then just click on Create, again this is going to take at least 30 mins to be created.
21. Once it is deployed then you need to go to User VPN configuration and download the virtual WAN user VPN profile.

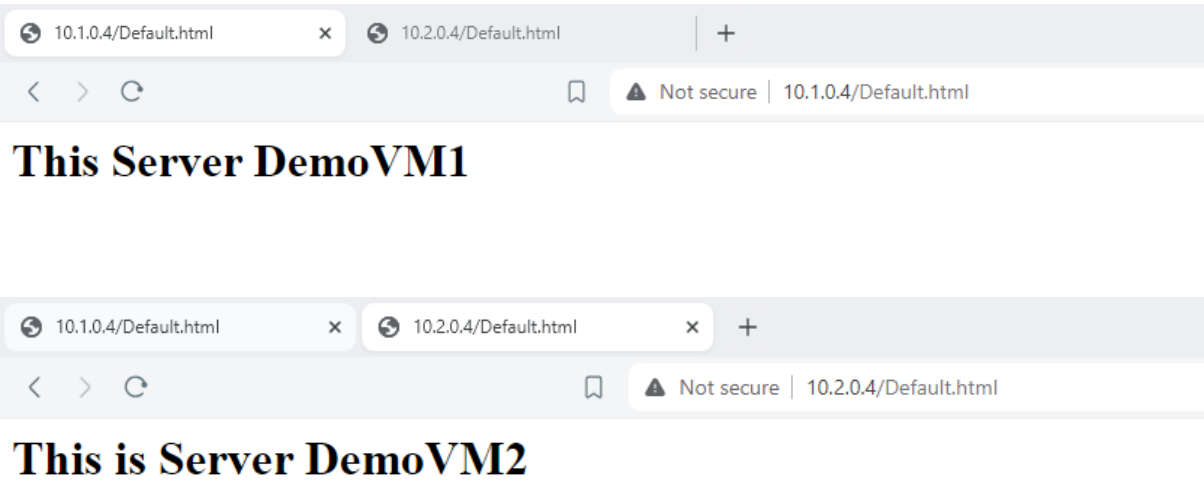


22. Once your file is downloaded then you need to extract it. In the extracted folder you will see that you have different packages to install from. Choose Windows AMD 64.



23. Once the file is installed, then in your laptop you need to search for VPN settings and you need to click on connect.

24. Once it is connected, now you need to copy the private IP addresses of both the VMs and paste then into a new browser or tab and make sure that you append the default html page.



25. Once you are done just delete all of the resources.