Cloud Virtual Network Setup

This playbook outlines the procedure for creating and managing virtual networks within a cloud environment. The aim is to establish secure communication channels between various cloud services.

Step 1: **Plan Network**

Determine the network's structure, including address spaces, subnets, and regions where the services will be deployed. Consider security policies, access control, and whether you need a multi-tier network.

Step 2: **Cloud Provider**

Choose a cloud provider that supports the desired network configurations and services. Review their networking services and understand the customizability they offer for virtual networks.

Step 3: **Create VNet**

Using the cloud provider's interface or CLI, create a new Virtual Network (VNet), specifying the selected address space, region, and any other required configuration settings.

Step 4: **Configure Subnets**

Within the Virtual Network, create subnets for different purposes (e.g., web, application, database tiers) and assign them appropriate address ranges within the VNet's address space.

Step 5: **Set Up Security**

Configure Network Security Groups (NSGs) or equivalent firewall rules to control traffic to and from each subnet. Specify rules based on the principle of least privilege.

Step 6: **Connect Services**

Link various cloud services to the virtual network by associating them with a particular subnet. Ensure the services have the necessary configurations to communicate securely.

Step 7: **Deploy Gateways**

If external connectivity is required (e.g., from on-premises networks), deploy VPN gateways or express routes as necessary and configure them according to your connectivity needs.

Step 8: **Test Network**

Perform connectivity tests between various components and services within the virtual network. Verify that security measures work as intended and that there is appropriate segmentation.

Step 9: **Monitor & Manage**

Use network monitoring tools provided by the cloud provider to continuously monitor network performance and security. Manage and adjust settings as needed to optimize for performance and cost.

General Notes

Documentation

Keep comprehensive documentation for network configurations, policies, and security rule sets for compliance and operational needs.

Backup

Implement backup strategies for network configurations to facilitate quick recovery in case of failures or unintended changes.

Compliance

Ensure that the network setup complies with industry regulations and standards applicable to your organization's operations.