Ubona Deployment Prerequisites in Azure Subscription

This document outlines the necessary prerequisites for deploying Ubona services in the Optum's Azure subscription.

1. Azure Subscription

- A dedicated **Azure subscription** must be created and available for Ubona deployment.
- Ensure billing and access policies are properly configured.

2. Compute and Networking Quotas

Verify and ensure quota availability for the following resources:

VM Size Quotas:

VM Size	Required
Standard_B2s	✓
Standard_D4as_v4	✓
Standard_DS2_v2	✓

> **Action**: Confirm these VM quotas are available in the **intended region** of deployment.

3. CIS Hardened Image Subscription

- The subscription must be **subscribed to CIS Hardened Images** for Rocky Linux 9:
  - **Publisher**: Center for Internet Security
  - **Plan ID**: `cis-rockylinux-9-l1-gen2`
- All Ubona VMs will be deployed using this hardened image via Terraform.

4. Azure Blob Storage

A dedicated Azure **Storage Account** must be created to house Ubona-related data artifacts. This storage will be used across deployment, monitoring, and auditing functions.

- The Storage Account must include the following **containers**:
  - `logs`: For storing application, infrastructure, and diagnostic logs.
  - `tfstate`: To store Terraform state files.
    ➤ Ensure **state locking** and **versioning** are enabled (e.g., via blob lease or Azure backend settings).
  - `recordings`: To store audio/video recordings or data captures relevant to Ubona's functionality.

5. Azure Access for Ubona User

- A **dedicated Azure AD user** (Ubona automation user) must have:

Required Permissions

1. **Subscription Level**:
   - `Contributor` role on the subscription
2. **Storage Account (Access to Storage account created in Step 4)**:
   - `Storage Blob Data Contributor` on the storage account for state file and recording operations
   - `Storage Account Contributor` for managing storage account settings
3. **Key Vault (within subscription)**:
   - `Key Vault Secrets User` at minimum for reading secrets during deployment
   - `Key Vault Administrator` to create and manage Key Vault and its secrets
4. **Compute**:
   - `Virtual Machine Contributor` for creating and managing virtual machines
   - `Shared Image Gallery Contributor` for accessing the CIS image gallery
5. **OpenAI Integration and Speech Services Integration**:
   - `Cognitive Services Contributor` for creating and managing OpenAI/Speech Service resources

Note: This user will be used by Terraform to deploy IaaS resources into the Optum's environment.

6. MySQL Flexible Server (POC-Specific Deployment)

As part of the POC, the **MySQL Flexible Server** required for Ubona will **not be provisioned through Terraform** and will instead be deployed manually.

- This server must be **launched via Azure Console** by the **Optum team**, with deployment parameters and guidance provided by the Ubona team.
- The deployment should be done after all other Ubona resources have been provisioned using Terraform.
- Configuration details (e.g., SKU, backup, redundancy, firewall rules) will be shared by Ubona to ensure compatibility and integration with the deployed infrastructure.

> 💡 Ensure that:
>
> - The server is placed in the same **resource group** or **virtual network**.
> - Required **firewall or VNet integration** is configured to allow internal communication with Ubona services.
> - Admin credentials or access policies are managed securely, ideally referencing **Azure Key Vault**.