Multimodal Reasoning AI Agent 🧠

Upload an image and provide a reasoning-based task for the AI Agent. The AI Agent will analyze the image and respond based on your input.

Upload Image

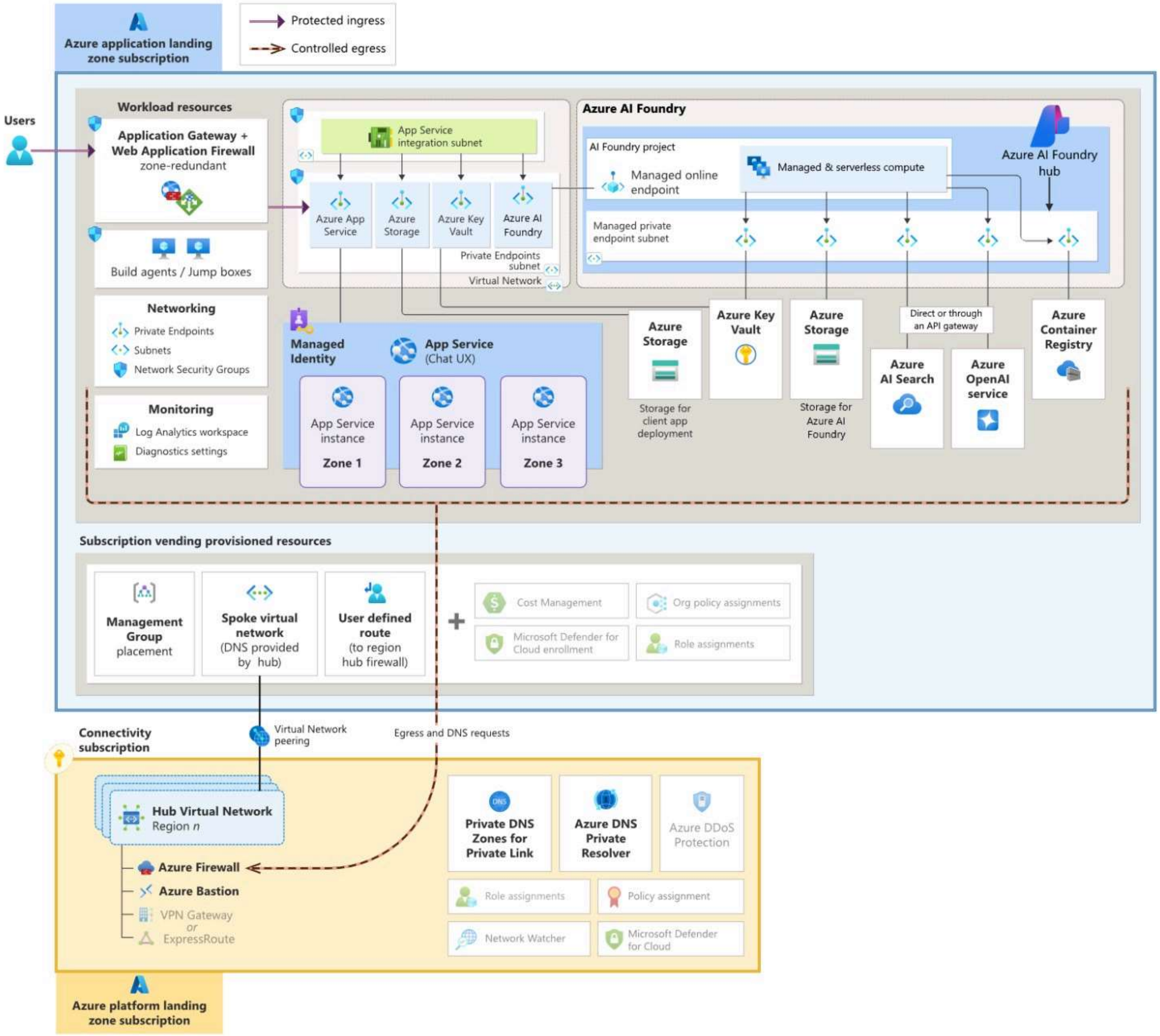
Drag and drop file here

Limit 200MB per file • JPG, JPEG, PNG

Browse files

azure-openai-baseline-landing-zone.png 216.5KB

×



Uploaded Image

Enter your task/question for the AI Agent:

explain this architecture

Analyze Image

AI Response:

This diagram illustrates a well-structured Azure application landing zone with a focus on security, scalability, and integration with Azure AI services. Let's break down the architecture section by section:

1. User Interaction and Protected Ingress:

- **Users:** The entry point is through users accessing the application.
- **Application Gateway + Web Application Firewall (WAF):** This is the protected ingress point. It acts as a reverse proxy, load balancer, and provides web application security by filtering malicious traffic. This is a zone-redundant setup for high availability.

2. Workload Resources (Azure Application Landing Zone Subscription):

- **Build agents / Jump boxes:** These are likely virtual machines used for development, deployment, and administrative tasks within the environment.
- **Networking:**
    - **Private Endpoints:** This indicates that many of the resources are accessed privately within the virtual network, enhancing security by preventing public exposure.
    - **Subnets:** The virtual network is segmented into subnets for better organization and security. The diagram highlights an "App Service integration subnet" and a "Private Endpoints subnet" within the main Virtual Network.
    - **Network Security Groups (NSGs):** These are used to filter network traffic in and out of subnets and network interfaces, providing granular control over network security.
- **Monitoring:**
    - **Log Analytics workspace:** This is where logs and metrics from various Azure resources are collected and analyzed for monitoring and troubleshooting.
    - **Diagnostics settings:** Configured on resources to send their logs and metrics to the Log Analytics workspace.
- **App Service (Chat UX):** This is the core application platform, likely hosting a chat user interface.
    - **App Service instances (Zone 1, Zone 2, Zone 3):** The application is deployed across multiple availability zones for high availability and resilience against zonal failures.
- **Azure App Service:** The specific Azure service used to host the application.
- **Azure Storage:** Used for general-purpose storage needs of the application.
- **Azure Key Vault:** Securely stores secrets, keys, and certificates used by the application.

- **Azure AI Foundry:** This section represents the integration with Azure's AI capabilities.
  - **AI Foundry project:** Represents a specific project within Azure AI Foundry.
  - **Managed online endpoint:** Provides a scalable and managed endpoint for deploying and serving AI models.
  - **Managed & serverless compute:** Indicates that the AI Foundry project leverages managed compute resources, likely Azure Machine Learning Compute or similar, for training and inference.
  - **Managed private endpoint subnet:** A dedicated subnet for private access to the AI Foundry resources.
- **Managed Identity:** Used by the App Service to securely access other Azure resources (like Key Vault and potentially AI services) without needing to manage credentials directly.

3. Azure AI Foundry Details:

- **Azure Storage (Storage for client app deployment):** Used to store artifacts or data related to the client application.
- **Azure Key Vault:** Potentially a separate Key Vault instance for securely managing secrets and keys specifically for the AI Foundry project.
- **Azure Storage (Storage for Azure AI Foundry):** Storage account for data used by the AI Foundry project, like training data or model artifacts.
- **Azure AI Search:** Provides a managed search service, likely used for indexing and searching data related to the AI application.
- **Azure OpenAI service:** Integration with Azure OpenAI to leverage powerful language models for the chat application. This connection can be direct or through an API gateway.
- **Azure Container Registry:** Used to store Docker images for the application or AI models.
- **Azure AI Foundry hub:** A central management and collaboration platform for AI projects within the organization.

4. Subscription Vending Provisioned Resources:

This section outlines resources that are likely provisioned and managed at a higher level, often as part of a platform team's responsibility, and shared across different application landing zones.

- **Management Group placement:** Highlights the organizational structure and how subscriptions are grouped.
- **Spoke virtual network (DNS provided by hub):** This represents the virtual network where the application resources reside. It's a "spoke" in a hub-and-spoke network topology, meaning it connects to a central "hub" virtual network for shared services. It also indicates that DNS resolution is managed by the hub.
- **User defined route (to region hub firewall):** Network traffic leaving the spoke virtual network is routed through a central firewall in the hub virtual network for security inspection.
- **Cost Management:** Tools and processes for tracking and managing Azure costs.
- **Microsoft Defender for Cloud enrollment:** Integration with Azure's cloud security posture management and threat detection service.

- **Org policy assignments:** Organization-level policies enforced on the subscription.
- **Role assignments:** Managing access and permissions to resources within the subscription.

5. Connectivity Subscription:

This subscription houses the central networking infrastructure and shared services.

- **Hub Virtual Network (Region n):** The central point of connectivity for the Azure environment.
- **Azure Firewall:** A managed, highly available network firewall service to inspect and control network traffic between subnets and external networks.
- **Azure Bastion:** Provides secure RDP/SSH access to virtual machines within the virtual network without exposing them directly to the public internet.
- **VPN Gateway or ExpressRoute:** Enables secure hybrid connectivity to on-premises networks.
- **Azure platform landing zone subscription: I**ndicates this connectivity subscription is part of a larger platform setup.

6. Egress and DNS Requests:

- **Virtual Network peering:** Establishes a network connection between the hub and spoke virtual networks, allowing resources in each network to communicate with each other privately.
- **Private DNS Zones for Private Link:** Used for resolving private endpoint addresses within the virtual network.
- **Azure DNS Private Resolver:** Enables querying of private DNS zones from on-premises networks or other Azure virtual networks.
- **Azure DDoS Protection:** Protects the public IP addresses of Azure resources from distributed denial-of-service attacks.
- **Role assignments, Policy assignment, Network Watcher, Microsoft Defender for Cloud:** These are additional services for security, governance, monitoring, and threat detection at the connectivity layer.

In summary, this architecture represents a secure and scalable Azure application landing zone. Key features include:

- **Security:** Strong emphasis on security with Application Gateway + WAF, private endpoints, Azure Firewall, NSGs, and Microsoft Defender for Cloud.
- **High Availability:** Zone-redundant Application Gateway and multi-zone deployment of App Service.
- **Scalability:** Leveraging Azure App Service and managed compute for AI services.
- **Centralized Networking:** Hub-and-spoke topology for managing connectivity and security.
- **AI Integration:** Seamless integration with Azure AI Foundry, OpenAI, and AI Search.
- **Managed Services:** Utilizing managed services like Azure App Service, Key Vault, and Azure AI services to reduce operational overhead.

This detailed explanation should give you a comprehensive understanding of the architecture depicted in the diagram.