@startuml

title Immuta Platform on Azure - Deployment Diagram

node "Azure" {

frame "Networking" {

node "Immuta VNet" {

[Immuta Application (AKS)]

[Metadata Database (PostgreSQL)]

[Elasticsearch (ISV)]

}

node "Shared Services VNet" {

[Blob Storage]

component "Network Security Groups (NSGs)" as NSGs\_Shared

}

}

frame "Security" {

component "Azure AD" as AAD

component "Key Vault" as KeyVault

component "App Gateway with WAF" as WAF

}

frame "Monitoring and Threat Protection" {

component "Azure Monitor" as Monitor

component "Microsoft Defender" as Defender

}

}

frame "Snowflake and Data Consumers" {

component "Snowflake" as Snowflake

actor "Data Consumers" as DataConsumers

}

actor "Immuta Admins" as ImmutaAdmins

' Connections and Relationships

AAD --> ImmutaAdmins : "Authenticates"

AAD --> DataConsumers : "Authenticates"

ImmutaAdmins --> [Immuta Application (AKS)] : "Manage Policies"

AAD --> [Immuta Application (AKS)] : "Authenticates"

KeyVault --> [Immuta Application (AKS)] : "Secures Secrets"

WAF --> [Immuta Application (AKS)] : "Routes Secure Traffic"

[Immuta Application (AKS)] --> [Metadata Database (PostgreSQL)] : "Policy Queries"

[Immuta Application (AKS)] --> [Elasticsearch (ISV)] : "Metadata Indexing"

[Immuta Application (AKS)] --> [Blob Storage] : "Stores Configurations"

[Immuta Application (AKS)] --> Snowflake : "Applies Policies"

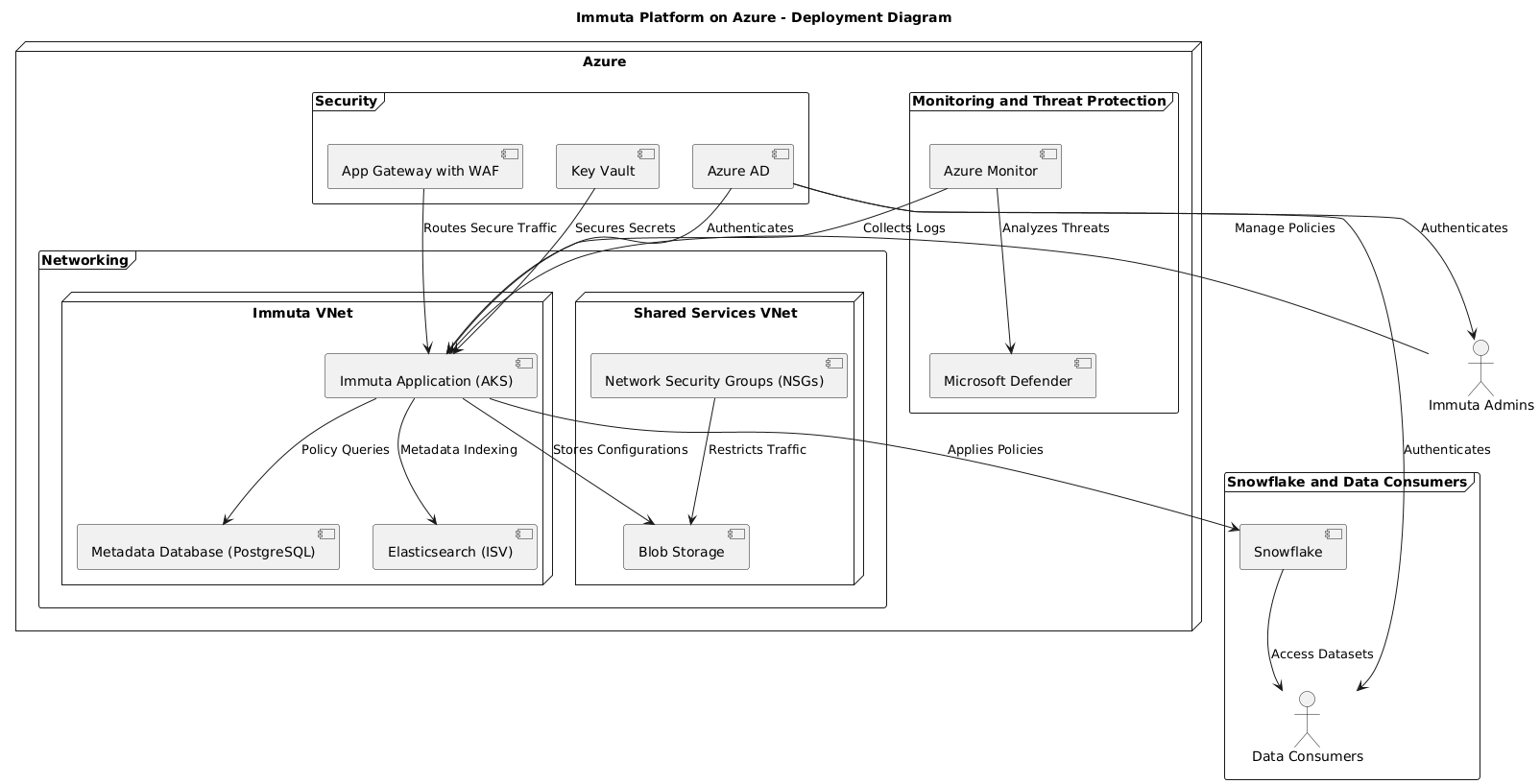
Snowflake --> DataConsumers : "Access Datasets"

Monitor --> [Immuta Application (AKS)] : "Collects Logs"

Monitor --> Defender : "Analyzes Threats"

NSGs\_Shared --> [Blob Storage] : "Restricts Traffic"

@enduml



### **Components**

|  |  |  |
| --- | --- | --- |
| **Component** | **Purpose** | **Details** |
| **Immuta Application (AKS)** | Central application enforcing data governance policies on Snowflake datasets. | Hosted on Azure Kubernetes Service (AKS) for scalability and high availability. |
| **Metadata Database (PostgreSQL)** | Stores Immuta policies, metadata, and configurations. | Deployed as Azure Database for PostgreSQL with encryption at rest. |
| **Elasticsearch (ISV)** | Enables fast metadata and policy indexing for Immuta. | Provided via Elastic Cloud as an ISV solution on Azure. |
| **Blob Storage** | Stores configurations, logs, and other temporary files for Immuta. | Secured with Azure NSGs and private endpoints. |
| **Azure AD** | Authenticates users and provides single sign-on (SSO). | Immuta Admins and Data Consumers are authenticated through Azure AD. |
| **Key Vault** | Secures secrets and manages encryption keys. | Used for storing sensitive configurations and keys required by Immuta components. |
| **App Gateway with WAF** | Protects and routes HTTP(S) traffic to Immuta. | Provides ingress filtering with web application firewall functionality. |
| **Azure Monitor** | Collects logs and metrics from Immuta and related services. | Logs forwarded to Defender for threat analysis. |
| **Microsoft Defender** | Provides threat detection and response capabilities. | Integrated with Azure Monitor to analyze logs for security incidents. |
| **Snowflake** | Data warehouse for storing governed datasets. | Policies are dynamically applied by Immuta. |
| **Data Consumers** | Users (analysts, data scientists) accessing Snowflake datasets. | Authenticated via Azure AD. |
| **Immuta Admins** | Manage Immuta policies and configurations. | Authenticated via Azure AD. |
| **NSGs (Network Security Groups)** | Enforce network segmentation and restrict unauthorized access. | Applied to subnets and services in the Immuta solution. |

Inherent Risk Assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk** | **Description** | **Drivers** | **Impact** | **Controls (CAD ID - CAD Name)** | **Questions** |
| **Unauthorized Data Access** | Users gain unauthorized access to sensitive datasets due to misconfigured access policies. | - Misconfigured ABAC or RBAC policies.  - Inadequate identity provisioning and reviews. | - Breach of confidentiality.  - Regulatory non-compliance.  - Loss of trust. | CT-115088 - Identity Access Requests are Approved.  CT-171062 - Role Management.  CT-115149 - User Access Reviews are Performed. | - What identity provisioning and deprovisioning processes are in place?  - Are access reviews conducted periodically? |
| **Data Exfiltration** | Sensitive data is exfiltrated through unmonitored channels or improper use of privileged accounts. | - Lack of DLP controls.  - Weak monitoring of data flows.  - Excessive privileges granted to users. | - Breach of sensitive data.  - Financial and reputational damage.  - Regulatory penalties. | CT-115148 - Data Encryption.  CT-115148 - Sensitive Data Masking.  CT-115162 - System Logging, Monitoring, and Alerting. | - Is data leakage prevention (DLP) configured for sensitive data?  - How are data flows monitored and anomalies detected? |
| **Privileged Account Misuse** | Abuse of privileged accounts results in unauthorized changes to policies or access controls. | - Insufficient privileged access monitoring.  - Temporary privileged access not properly logged or reviewed. | - Unauthorized policy changes.  - Disruption of governance mechanisms. | CT-115747 - Privileged Access Temporary Use.  CT-115747 - Break Glass Activity Reporting.  CT-115747 - Privileged Account Multi-Factor Authentication. | - What privileged account monitoring mechanisms are in place?  - Are break glass activities reviewed periodically? |
| **Key Compromise** | Cryptographic keys are exposed or misused, compromising the security of encrypted data. | - Weak key management policies.  - Lack of HSM usage.  - Improper key storage or rotation. | - Exposure of encrypted sensitive data.  - Loss of trust in solution security. | CT-187470 - Secure Key Storage.  CT-187470 - Key Export Policies.  CT-115148 - Encryption in Transit. | - Is a Key Management Plan (KMP) implemented and reviewed periodically?  - Are HSMs used for key storage? |
| **Configuration Drift** | Deviation from approved configurations introduces vulnerabilities. | - Lack of baseline configuration monitoring.  - Unauthorized configuration changes.  - Manual updates. | - Increased attack surface.  - Higher likelihood of breaches. | CT-115182 - Configuration Drift Monitoring.  CT-115182 - Hardened Baseline Configurations.  CT-115182 - Access to Baseline Images. | - How is configuration drift monitored and corrected?  - Are baseline configurations documented and enforced? |
| **Data Leakage through APIs** | Exploitation of Immuta APIs leads to unauthorized data access or exfiltration. | - Insufficient API authentication.  - Improper API rate limiting and access controls.  - Lack of logging for API activity. | - Breach of sensitive data.  - Compliance violations.  - Financial penalties. | CT-115083 - API Authentication Logging.  CT-188022 - API Specification Enforcement.  CT-188022 - API Endpoint Security. | - Are Immuta APIs protected with authentication and rate limiting?  - Are API activities logged and monitored? |
| **Service Downtime due to DDoS Attacks** | Distributed Denial of Service (DDoS) attacks disrupt Immuta services, affecting availability and policy enforcement. | - Lack of DDoS protection for public-facing endpoints.  - Open network access rules.  - Insufficient segmentation. | - Loss of service availability.  - Business continuity disruptions. | CT-187461 - Hostile Zone Protection.  CT-265275 - Secure Internet Traffic.  CT-187461 - Network Segmentation. | - Are public-facing endpoints protected by DDoS solutions?  - What segmentation policies are applied to VNets? |
| **Insufficient Logging and Monitoring** | Lack of centralized logging and alerting mechanisms delays detection of unauthorized activity or breaches. | - Logs not onboarded to central monitoring systems.  - Ineffective alert tuning.  - Lack of operational visibility. | - Delayed breach detection.  - Missed compliance requirements.  - Prolonged recovery times. | CT-115162 - Real-Time Alerting.  CT-115162 - Enterprise Logging Integration.  CT-115162 - Alert Escalation Policies. | - Are logs centralized and ingested into Azure Monitor or Sentinel?  - Are alerts reviewed and fine-tuned? |
| **Non-Compliance with Regulatory Standards** | Immuta policies and configurations fail to meet requirements set by GDPR, NZ Privacy Act, or APRA standards. | - Inadequate access control.  - Lack of logging for audit purposes.  - Unclassified datasets. | - Fines and penalties.  - Reputational damage.  - Loss of customer trust. | CT-115149 - User Access Reviews are Performed.  CT-188029 - Data Classification Standards.  CT-115286 - Vulnerability Reporting. | - How is regulatory compliance validated and documented?  - Are datasets classified according to standards? |
| **Backup and Recovery Failures** | Failure to restore critical data during outages compromises business continuity. | - Insufficient backup testing.  - Lack of encryption for backup data.  - Unmonitored backup failures. | - Permanent data loss.  - Disruption of critical services. | CT-115242 - Backup Status Monitoring.  CT-115242 - Data Restoration Testing.  CT-115242 - Backup Retention Policies. | - Are backups encrypted and tested regularly?  - How are backup failures identified and resolved? |