**Azure**

|  |  |  |
| --- | --- | --- |
| Azure Component | Security Configuration | Recommended Settings/Values |
| Azure Kubernetes Service (AKS) | - Enable Private Endpoint for API server. - Use Network Policies for pod communication. - Enable Role-Based Access Control (RBAC) for cluster management. - Enable Auto-Repair and Cluster Autoscaler. | Private Endpoint: Enabled Pod Network Policies: Enforced RBAC: Configured for Cluster Management Auto-Repair: Enabled Autoscaler: Enabled |
| Azure Database for PostgreSQL | - Enable Encryption at Rest. - Restrict access to Private Endpoint only. - Enable Active Geo-Replication for DR. - Configure RBAC for database administrators. | Encryption: Enabled with CMKs Access: Private Endpoint Only Geo-Replication: Enabled RBAC for DB Management: Configured |
| Azure Blob Storage | - Enable Immutable Storage. - Configure NSGs to limit access. - Use Private Endpoints. - Enable Geo-Redundant Storage (GRS). - Enforce RBAC for storage management. | Immutable Storage: Enabled (WORM) NSG Rules: Least-Privilege Access Private Endpoints: Enabled GRS: Enabled RBAC: Configured for Admin Roles |
| Azure Key Vault | - Enable Private Endpoint. - Enforce Automatic Key Rotation. - Use CMKs for encryption. - Enable Soft Delete and Purge Protection. - Configure RBAC for Key Vault management. | Private Endpoint: Enabled Key Rotation: Every 90 Days Encryption: CMKs Soft Delete and Purge Protection: Enabled RBAC: Configured for Key Administrators |
| Azure Container Registry (ACR) | - Enable Image Scanning with Microsoft Defender. - Restrict access via NSGs and Private Endpoints. - Enforce RBAC for image management (push/pull). | Defender for Containers: Enabled Private Endpoints: Enabled NSGs: Least-Privilege Access RBAC for Image Operations: Configured |
| Application Gateway with WAF | - Enable OWASP Top 10 Rules. - Configure Rate Limiting for DDoS Protection. - Enable HTTPS Termination. - Configure RBAC for Gateway Management. | WAF Rules: Enabled (OWASP Top 10) Rate Limiting: Configured HTTPS Termination: Enabled RBAC for Gateway Admins: Configured |
| Azure Monitor | - Enable Diagnostic Settings. - Forward Logs to Event Hubs for SIEM Integration. - Configure Log Retention for 1 Year. - Apply RBAC for monitoring operations. | Diagnostic Settings: Enabled Log Forwarding: Event Hubs Log Retention: 1 Year RBAC: Configured for Monitoring Roles |
| Event Hubs | - Restrict Access via Private Endpoints. - Enable Geo-Redundancy for Disaster Recovery. - Configure RBAC for Event Hub management. | Private Endpoints: Enabled Geo-Redundancy: Enabled RBAC for Event Hub Admins: Configured |
| Microsoft Defender for Cloud | - Enable Defender Modules for all Resources. - Configure Threat Detection Alerts. - Set Secure Score Monitoring for Misconfigurations. - Apply RBAC for security operations. | Defender for Containers, Key Vault, Storage, and SQL: Enabled Threat Alerts: Configured Secure Score: Monitored RBAC for Security Teams: Configured |
| Azure Active Directory (AAD) | - Enforce Multi-Factor Authentication (MFA). - Apply Conditional Access Policies. - Configure Privileged Identity Management (PIM) with RBAC for admin roles. | MFA: Mandatory Conditional Access: Enforced for all admin accounts PIM and RBAC for Admins: Configured |
| Network Security Groups (NSGs) | - Implement Least-Privilege Rules. - Restrict Subnet Communication. - Configure RBAC for NSG rule management. | Inbound Rules: Allow Specific Ports (e.g., HTTPS 443, PostgreSQL 5432) Outbound Rules: Deny All Except Specific Endpoints RBAC for NSG Management: Configured |
| Snowflake (via PrivateLink) | - Use PrivateLink for Secure Connectivity. - Enforce Strict Policy Evaluation. - Configure Role-Based Access Control (RBAC) for dataset management. | PrivateLink: Enabled Policy Evaluation: Strict RBAC for Dataset Management: Configured |
| Exabeam SIEM | - Integrate with Event Hubs. - Enable Threat Correlation for Access Logs. - Configure RBAC for SIEM administration and incident management. | Integration: Event Hubs Threat Correlation: Enabled RBAC for SIEM Operations: Configured |

**RBAC Recommendations for Management Operations**

1. **Principle of Least Privilege:** Assign roles with only the permissions necessary for specific tasks (e.g., Reader, Contributor).
2. **Azure RBAC Built-in Roles:** Use predefined roles where possible (e.g., Storage Account Contributor, Kubernetes Cluster Admin) and create custom roles only when needed.
3. **Privileged Identity Management (PIM):** Enable PIM to control elevated privileges for Azure resources, ensuring Just-in-Time (JIT) access.
4. **Audit Role Assignments:** Log and monitor RBAC changes in Azure Monitor to detect misconfigurations or privilege escalations.