CDW Documentation

Azure Key Vault Best Practices

Azure Key Vault Best Practices

Overview

Azure Key Vault is a cloud service for securely storing and accessing secrets, keys, and certificates. To maximize security, it's critical to follow industry-standard and Microsoft-recommended practices.

---

1. Access Control

Use Azure RBAC (Role-Based Access Control)

- Prefer **Azure RBAC** over Access Policies when possible for granular and scoped access control.
- Assign least-privilege roles:
  - **Key Vault Reader** for read-only access
  - **Key Vault Contributor** for full management (no data plane)
  - **Secret/Key/Certificate Operator** roles for specific operations

Enable Role Assignments at the Right Scope

- Assign roles at **resource group** or **vault level**, not subscription-wide.

Use Managed Identities

- Use **system-assigned or user-assigned managed identities** for Azure resources needing access.
- Avoid hardcoded credentials in code.

---

2. Secrets, Keys, and Certificates Management

Enable Soft Delete

- Protects against accidental or malicious deletion.
- Retains deleted items for a default period (up to 90 days).

Enable Purge Protection

- Prevents permanent deletion of Key Vault objects before retention period ends.

Set Expiration Dates

- Apply expiry dates to secrets, keys, and certificates.
- Monitor expiration and renew proactively.

Use Versioning

- Secrets and keys are versioned automatically—don’t overwrite in-place.
- Use new versions for each update.

---

3. Monitoring and Auditing

Enable Logging

- Turn on **Azure Monitor diagnostic logs**:
  - AuditEvent (access requests)
  - AllMetrics (performance)
- Send logs to:
  - **Log Analytics**
  - **Event Hubs**
  - **Storage Accounts**

Set Alerts

- Configure **alerts** for:
  - Unauthorized access attempts
  - Secrets/keys expiring soon
  - High-frequency access patterns

---

4. Networking and Access Restrictions

Use Private Endpoints

- Enable **Private Link** to restrict Key Vault access over Azure backbone only.
- Avoid exposing the vault publicly.

Use Firewall Rules

- Restrict access to **specific trusted IPs** or **VNet subnets**.
- Set **“Allow trusted Microsoft services”** only if required.

5. 🔐 Encryption and HSM

🔑 Use Customer-Managed Keys (CMK)

- For compliance, encrypt vault data using your own **Key Encryption Key (KEK)**.

🧱 Use Premium Tier for HSM-backed Keys

- Required for high-assurance applications (e.g., FIPS 140-2 Level 3).
- Supports **Managed HSM** for isolated key storage.

---

6. ⚙️ Automation and Governance

📜 Use Azure Policy

- Enforce standards like:
  - Vaults must have soft delete enabled
  - Disallow public network access
  - Require private endpoints

🔄 Automate Secret Rotation

- Use **Key Vault Event Grid integration** or **Azure Functions** to auto-rotate secrets and certificates.

🧹 Regularly Review Access

- Audit who has access to Key Vault and prune unnecessary roles or policies.

---

7. 🔐 Multi-Factor Authentication (MFA)

- Require **MFA** for all users with control-plane (management) access.
- Use **Conditional Access Policies** to enforce strong authentication and device compliance.

Summary Checklist

Practice	Status
Soft Delete + Purge Protection enabled	
Public access disabled (Private Link preferred)	
RBAC roles scoped to least privilege	
Secrets and keys have expiration dates	
Logging and alerting configured	
MFA + Conditional Access for admins	

AI Knowledge