Technical Solution Brief

Windows 2022 - Certificate Management

September 3, 2025

Next Orbit Windows Server 2022 – Deep Technical Optimization & Image Baking Strategy

success@nextorbit.co | nextorbit.co | +1-833-ORBIT-00

How AKV Client Is Implemented

- **At Build Time (Image Creation):**
  We intentionally **do not bake Key Vault secrets or certificates into the image**. Instead, the images are pre-staged with the **AKV VM extension capability** configured as an integration point.
    - This ensures the image is clean, immutable, and not tied to a specific vault or certificate at build time.
    - It avoids the anti-pattern of hardcoding Key Vault URIs or secrets directly into templates.
- **At Deploy Time (VM Provisioning):**
  The **Azure Key Vault VM extension** (`KeyVaultForWindows`) is deployed alongside the VM.
    - It fetches certificates from AKV into the **LocalMachine\My** certificate store.
    - It handles **auto-renewal** transparently, checking AKV on a polling interval (default ~1 hour).
    - Certificates are linked automatically to renewal events, ensuring continuity without manual intervention.
- **Post-Deployment Binding:**
  A **post-config PowerShell script** (`Bind-SqlServerCertificate.ps1`) is included in the solution:
    - It reads the desired certificate **thumbprint** from the LocalMachine\My store.
    - It binds the certificate to the SQL instance (MSSQLSERVER or named instance) via registry and restarts the SQL service.

- This step ensures SQL Server endpoints (TDS, AlwaysOn listeners, etc.) use the AKV-provided certificate.

Security Advantages

- **Separation of Concerns:** Certificates are never in the image → reduces exposure if the image is shared.
- **Managed Identity Authentication:** The AKV extension uses Managed Identity → no secrets in pipelines.
- **Continuous Renewal:** Automatic polling + renewal means certificates stay valid without manual ops.
- **Auditability:** Certificates remain in AKV, with full Key Vault logging and RBAC control.

Alignment with Immutability

- The image remains **immutable** (no secrets, no certs).
- Rotation is handled at runtime by AKV extension, outside of the baked image lifecycle.
- This respects the principle of "**build once, deploy many**" while still ensuring cert freshness.

Stability Benefits

- **No drift:** Every VM built from the golden image behaves identically, relying on AKV for cert material.
- **No outages:** Certificates are renewed automatically before expiry. SQL binding script ensures rebinds succeed.
- **Resilience:** If a cert is compromised or replaced, AKV pushes the new version without image rebuilds.

Time & Effort Saved

- **Without AKV:** Ops teams would manually issue, install, and rotate certs → ~30–60 minutes per SQL server, 4x a year.
- **With AKV client:** Cert rotation is automated, requiring **zero ops time** per renewal.
- **Estimated savings:** ~2–3 hours of manual effort saved per SQL server annually, plus reduction in human error risk.

Overall: Our methodology implements AKV integration **exactly as recommended by Microsoft** — clean images, runtime certificate retrieval, automated rotation, and SQL binding via script. It achieves immutability, security, and operational savings, while avoiding common pitfalls (baking secrets, drift, manual installs).
