Azure Landing Zone Blueprint for Qualys VM Snapshot Scanning

# 1. Reference Architecture (Well-Architected + Landing Zone)

The environment should follow Microsoft’s Cloud Adoption Framework (CAF) and Azure Well-Architected Framework. It consists of a centralized platform (hub) and multiple application landing zones (spokes). Key services include management groups, policy baselines, centralized logging, Defender for Cloud, hub-spoke networking, and shared services such as Bastion, PrivateLink, and Firewall.

# 2. Resources to Deploy (By Layer)

A. Tenant / Management: Management Groups, Azure Policy Initiatives, Azure AD App Registration for Qualys Connector.

B. Subscriptions: Platform subscription (hub + shared services), workload subscriptions (Dev/Test/Prod).

C. Networking: Hub VNet (Firewall, Bastion, Scanner subnet), Spoke VNets per environment with peering.

D. Security & Observability: Log Analytics workspace, diagnostics settings, Defender for Cloud enablement.

E. Image Management: Azure Compute Gallery for golden Windows/Linux images.

F. Qualys Components: Qualys Azure Connector and optional dedicated Qualys Virtual Scanner Appliance (VSA) VM.

# 3. RBAC (Roles)

For Qualys snapshot-based scanning, the Azure AD service principal requires:  
- Reader (enumerate resources)  
- Disk Snapshot Contributor (create/read disk snapshots)  
- Data Operator for Managed Disks (if export access is needed)  
  
For the Qualys VSA VM: Standard VM Contributor for self-management. Networking and firewall remain platform-owned.

# 4. Implementation Steps (Runbooks)

A. Prepare landing zone: Create management groups, apply policy baselines, create subscriptions, enable Defender, build hub/spoke VNets, configure Log Analytics, and create Compute Gallery.

B. Configure Qualys snapshot-based scanning: Register Azure AD app, assign RBAC roles, configure Qualys connector, enable snapshot-based scanning, schedule scans.

C. Deploy optional Qualys VSA VM: Place in hub scanner subnet, restrict network rules, register with Qualys, configure access to spokes.

# 5. Image-Level Guidance

Snapshot-based scanning works on any Azure VM with managed disks. No agents are needed. Ensure custom images are patched and versioned. For authenticated scans via the VSA, configure limited accounts with required privileges (WMI/WinRM for Windows, SSH with sudo for Linux) and store credentials securely in Azure Key Vault.

# 6. Operations, Safety, and Costs

- Schedule scans outside peak usage to minimize snapshot/storage load.  
- Use least privilege RBAC for Qualys connectors.  
- Restrict scanner VM outbound traffic only to required destinations.  
- Monitor snapshot storage costs and configure lifecycle management.  
- Consider Microsoft Defender for Cloud integrated vulnerability management for complementing Qualys scanning.

# 7. Suggested Repo Structure (Terraform/Bicep)

landing-zone/  
 platform/  
 hub-network/  
 policy/  
 logging/  
 defender/  
 subscriptions/  
 dev/ test/ prod/  
 spokes/  
 gallery/  
 keyvault/  
 security/  
 qualys-connector/  
 qualys-scanner-vm/

# Summary

This enterprise-grade landing zone blueprint aligns with Microsoft’s Well-Architected and CAF guidance, while integrating Qualys VM snapshot-based scanning. It provides a secure, scalable foundation for managing compliance and vulnerability assessment across Windows and Linux workloads in Azure.