–

**Capstone Project: Secure Multi-VNET IIS Log Processing on Azure**

# **Pipeline project for using Jenkins +Git + JMeter +Ansible**

**Project overview**

PREPARED BY:

PREPARED FOR:

**Version:** 1.0  
**Department:** Architect Department  
**Delivery:** End of Month

Table of Contents

[**1.** **The Project Summary** 3](#_Toc206250281)

[**2.** **The Proposed Solution** 3](#_Toc206250282)

[**3.** **High-Level Proposed Design** 3](#_Toc206250283)

[4. **Project Gantt chart** 4](#_Toc206250284)

[**5.** **Technologies Involved** 5](#_Toc206250285)

[**6.** **Business Value** 5](#_Toc206250286)

[**7.** **Steps for Execution** 6](#_Toc206250287)

[**8.** **Tentative Costing** 6](#_Toc206250288)

# **The Project Summary**

This project proposes a secure, cloud-native Azure-based architecture for log management and storage replication across two virtual networks (VNets). The design ensures separation of workloads, security via Private Endpoints and Azure Key Vault, and automation through Azure Functions. The solution provides a resilient, enterprise-grade architecture that can be extended to production workloads.

# **The Proposed Solution**

* Two Azure VNets are created to separate workloads:
* **VNet1:** Hosts two Azure Virtual Machines (VMs) that generate and store application/system logs in **Blob Storage1**.
* **VNet2:** Hosts **Blob Storage2**, the target for replicated logs from Blob Storage1.
* **Private Endpoints** ensure secure communication between VMs, Blob Storage, and Azure Functions without exposing resources to the public internet.
* **Azure Function** automates the replication of logs from Blob Storage1 (in VNet1) to Blob Storage2 (in VNet2).
* **Azure Key Vault** secures VM secrets, storage account connection strings, and Function access keys.
* **Management Groups & Resource Groups** enforce governance, cost management, and RBAC-based access control.

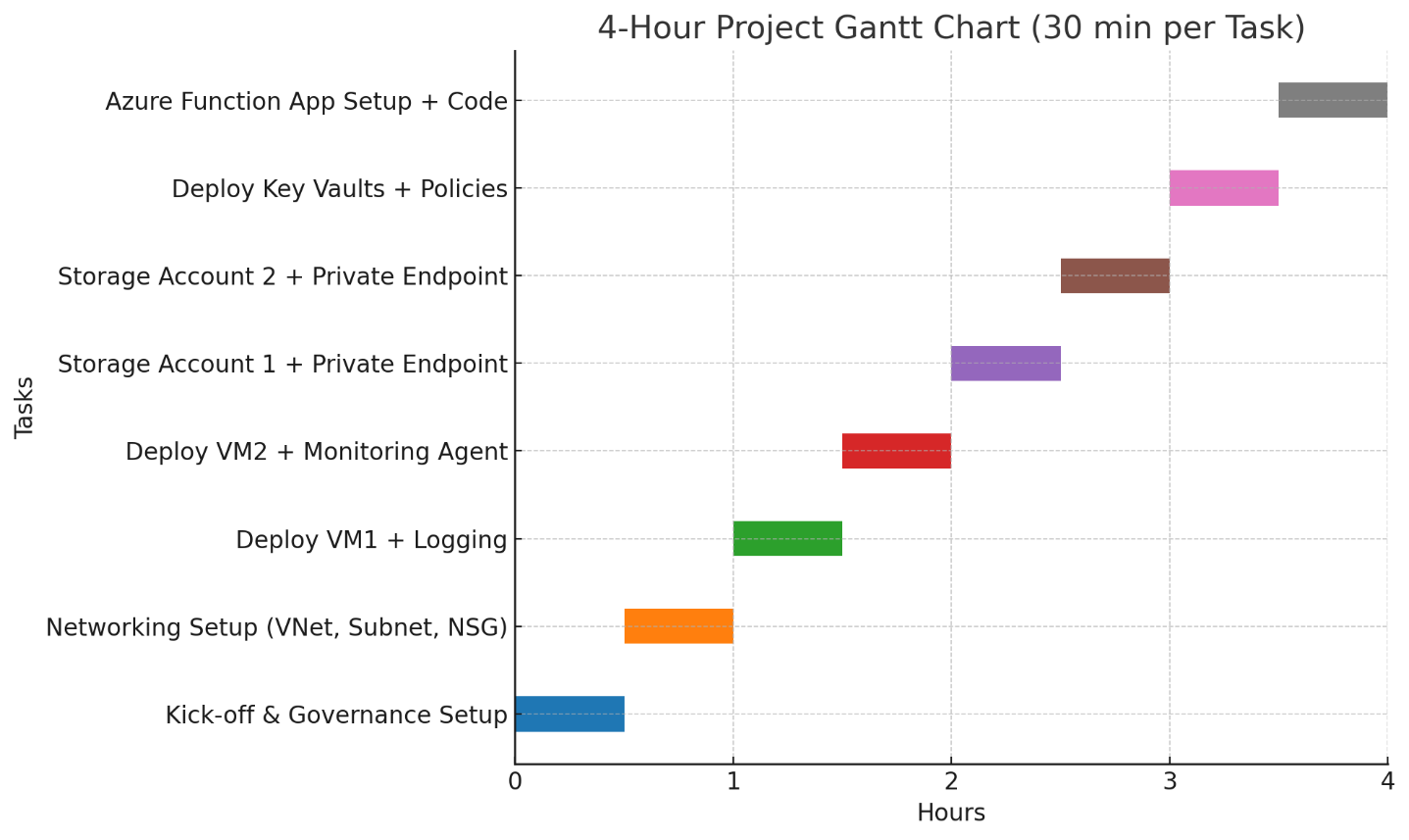
.

# **High-Level Proposed Design**

A diagram of a diagram

AI-generated content may be incorrect.

# **Project Gantt chart**



# **Technologies Involved**

| **Component** | **Azure Service Used** |
| --- | --- |

|  |  |
| --- | --- |
| Component | Azure Service Used |
| Networking | **Virtual Network (VNet1 & VNet2), Subnets, VNet Peering/Routing** |
| Compute (Log Source) | **Azure Virtual Machines (Windows/Linux)** |
| Storage (Primary) | **Azure Blob Storage1 (VNet1 with Private Endpoint)** |
| Storage (Replica) | **Azure Blob Storage2 (VNet2 with Private Endpoint)** |
| Automation | **Azure Function App** |
| Security | **Azure Key Vault, Private Endpoints, NSGs** |
| Governance | **Management Groups, Resource Groups, RBAC** |
| Monitoring | **Azure Monitor + Log Analytics Workspace** |

# **Business Value**

|  |  |
| --- | --- |
| Business Value | Description |
| Security | Private Endpoints + Key Vault protect data & secrets from exposure. |
| Scalability | Blob storage auto-scales; Azure Functions scale on demand. |
| Cost Optimization | Pay-as-you-go model with serverless automation reduces costs. |
| Operational Efficiency | Automated log replication removes manual intervention. |
| Governance & Compliance | Management Groups & RBAC align with enterprise IT policies. |
| Resilience | Multi-VNet architecture improves fault isolation & redundancy. |

# **Steps for Execution**

1. **Planning & Governance Setup**

* Define Management Groups, Resource Groups, RBAC roles, and naming conventions.

1. **Networking**

* Create VNet1 and VNet2 with subnets.
* Configure VNet Peering or VNet Routing between VNet1 and VNet2.

1. **Compute & Logging**

* Deploy two VMs in VNet1.
* Configure VM applications to send logs to Blob Storage1 (via Private Endpoint).

1. **Storage Setup**

* Create Blob Storage1 in VNet1 and Blob Storage2 in VNet2.
* Enable Private Endpoints for both storage accounts.

1. **Security**

* Deploy Azure Key Vault in each VNet to store secrets (VM credentials, storage keys, function keys).
* Configure NSGs and firewall rules for least-privilege access.

1. **Automation**

* Deploy Azure Function in VNet1 to replicate logs from Blob Storage1 → Blob Storage2.
* Secure Function with Key Vault references.

1. **Monitoring & Validation**

* Configure Azure Monitor & Log Analytics to track VM logs, Function execution, and storage replication.
* Validate log replication and security policies.

1. **Handover & Documentation**

* Document architecture, policies, and runbooks for operations.

# **Tentative Costing**

|  |  |  |  |
| --- | --- | --- | --- |
| Service / Resource | Quantity | Unit Cost (Approx.) | Est. Monthly Cost |
| Azure Virtual Machines | 2 × B2s (2 vCPU, 4 GB RAM) | ~$30 each | ~$60 |
| Blob Storage (Hot Tier) | 2 Accounts × 100 GB | ~$0.02/GB | ~$4 |
| Storage Transactions | ~1M ops/month | ~$0.05 per 10K | ~$5 |
| Private Endpoints | 2 Endpoints | ~$7.30 each | ~$15 |
| Azure Function (Consumption) | 1M executions/month | Free tier covers most PoC needs | ~$0 |
| Azure Key Vault | 2 Vaults | ~$1 per 10K operations | ~$3 |
| VNet Peering | Intra-region | ~$1 per VNet | ~$2 |
| Azure Monitor + Log Analytics | 5 GB ingested logs | ~$2.76/GB | ~$14 |
| Misc. (Bandwidth, Metadata, etc.) | - | - | ~$5 |

Total Estimated Cost: $110 – $120 (₹9K – ₹10K)