Hybrid Acronis & Microsoft Azure for Backup & DR

This strategy separates backup and DR functions across two different platforms and vendors.

Solution Architecture:

1. **On-Premises Backup (Local):**
    - **Software:** ACPC agents back up 3 servers and the Synology NAS to the **HPE StoreEasy 1660**.
2. **Offsite Backup (Cloud Storage):**
    - **Replication:** ACPC replicates backups to a cost-effective **Azure Blob Storage** container for long-term retention.
3. **Disaster Recovery (Cloud Replication):**
    - **Software: Azure Site Recovery (ASR)** is used to continuously replicate the 3 physical servers to Azure. The Synology NAS is NOT protected by ASR.
    - **DR Connectivity:** Your **Sophos appliance** will be configured with a Site-to-Site VPN to the designated Azure Virtual Network (VNet) for failover and failback traffic.
    - RPO: ASR's replication frequency can be configured to be as low as every few minutes for the three physical servers.
    - RTO: ASR's recovery plans orchestrate the failover process, allowing you to bring up the servers as Azure VMs within a 15-minute Recovery Time Objective (RTO).

On-Premises Deployment Requirements:

- **ASR Configuration Server:** A dedicated on-premises server (physical or VM) is **required**. It acts as the management hub for ASR replication.
    - *Minimum Specs: Windows Server 2016, 8 vCPU, 16 GB RAM, ~700 GB Disk Space.*
- **ASR Mobility Service Agent:** An agent that is pushed from the Configuration Server to each of the 3 physical servers being protected.
- **Acronis Agents:** Installed on servers for backup function only.
- **HPE StoreEasy 1660:** Racked, powered, and connected to the primary business network.
- **Network Configuration:**

- All protected machines and the HPE appliance require network access to each other for local backups.
- All protected machines require internet access to communicate with the Acronis Cloud management console and replicate data.
- Your **Sophos appliance** must be configured with a Site-to-Site VPN tunnel to your provisioned Azure Virtual Network Gateway.

Disaster Recovery Process & Caveat: Complex & Risky Physical Failback

While failover to Azure is robust, failback from an Azure VM to a new on-premises physical server is **not a supported, direct process**. It is a multi-stage manual, lengthy "Virtual-to-Physical" (V2P) conversion that requires significant technical expertise and carries a high risk of delay on failback when converting virtual to physical. Failback is from Azure to an on-prem VMware VM then convert the virtual disk to physical disk.

Billing & Cost Structure

Costs are fragmented across multiple services and vendors, with more variables during a disaster.

Cost Component	Description	Recurring Monthly Charges (RWF)
Monthly Recurring Cost (Backup)	Acronis Cyber Protect License:Covers 3 servers + 1 NAS. Acronis Cloud Storage: Pooled storage for offsite backup copies.	5,748,750
Monthly Recurring Cost (DR)	Azure Site Recovery License: Per-instance fee for each of the 3 protected servers and disk replication. Azure VPN Gateway.	2,092,500
Estimated Failover Compute Cost	Pay-as-you-go cost incurred ONLY during a disaster. Covers Azure VM runtime, managed disks, public IPs, and potential data egress fees. Based on 7 days (168 hours) of compute runtime per month.	2,216,250
Onsite Storage	HPE StoreEasy 1660 - NAS Server: Lease to own chargeable per month	1,500,000
Sub. Total		11,557,500
18% VAT		2,080,350
G.Total		13,637,850