# WSFC Stretch to AWS (Single-Subnet AG) — High-Level Plan

> Scope reminder: Extend an on‑prem Windows Server Failover Cluster (WSFC) hosting \*\*SQL Server Always On AG\*\* into \*\*AWS\*\* (single subnet in AWS). \*\*No DNN\*\*. Use a \*\*VNN listener\*\* fronted by an \*\*AWS Load Balancer\*\*. Keep focus tightly on the items below.

\*\*On‑prem\*\*

- Verify WSFC health and quorum (current: \*\*Node Majority\*\*), review recent cluster events.

- Confirm SQL Server Enterprise + AG enabled; note versions/patch (CU) for feature compatibility.

- Inventory DBs, RPO/RTO, log growth, and app connection strings.

- Open required ports to AWS (TCP 1433 for client, \*\*5022\*\* for AG endpoints, RDP/SSM as needed).

- Ensure reliable time sync and domain controller reachability for the new site.

- Backups validated (full + tlog); document rollback plan.

\*\*AWS (landing)\*\*

- Region selected; create / reuse \*\*VPC\*\* and \*\*single private subnet\*\* for SQL nodes (no public IPs).

- Hybrid link: \*\*Site‑to‑Site VPN\*\* (PoC) and/or \*\*Direct Connect\*\* with BGP; route tables updated.

- DNS: conditional forwarders or AD integration so both sides resolve each other.

- IAM/SSM baseline: Instance Profile for SSM Session Manager (no inbound RDP from Internet).

- AMIs: Windows Server (supported by SQL version); storage layout planned (EBS for data/log/tempdb).

- \*\*Connectivity\*\*: IPsec S2S VPN first; DX later for bandwidth. Keep VPN as failover.

- \*\*Routing\*\*: Summarized routes on‑prem; AWS route tables allow return to on‑prem.

- \*\*Security groups / firewalls\*\*: Least privilege. Allow: 1433 (NLB→SQL), 5022 (node↔node), AD/DNS/LDAP (domain join), custom health probe port if used.

- \*\*Name resolution\*\*: Route 53 resolver endpoints + conditional forwarders, or AD DNS replication.

- \*\*Time/AD\*\*: NTP parity; domain join AWS nodes to on‑prem AD.

- \*\*EC2 sizing\*\*: Start with parity to on‑prem (e.g., `m6i.large`/`r6i.large`), adjust via perf baselines.

- \*\*Disks\*\*: Separate EBS volumes for data/log/tempdb/backup. `io2` for log, `gp3` for data.

- \*\*OS prep\*\*: Install Failover‑Clustering feature; join domain; enable SSM.

- \*\*SQL prep\*\*: Install SQL Server; enable \*\*AlwaysOn\*\*; create AG endpoint on \*\*TCP 5022\*\*.

- \*\*Security\*\*: No public IPs; SSM for access; KMS‑encrypted EBS; tag all resources.

- Add AWS nodes to the existing \*\*WSFC\*\*.

- Change quorum from \*\*Node Majority\*\* to \*\*Node + File Share Witness\*\* (FSW on‑prem preferred) so the primary site retains majority during WAN blips.

- Manage node votes: give FSW a vote; consider clearing votes on DR side until cutover to avoid split‑brain. Keep \*\*Dynamic Quorum\*\* on.

- Use an \*\*AWS Network Load Balancer (NLB)\*\* on TCP \*\*1433\*\* with targets = SQL nodes.

- Health check: TCP 1433 or a \*\*custom health probe port\*\* that reports \*\*healthy only on the primary\*\* (via PowerShell/URL helper).

- Create the AG \*\*VNN listener\*\* in WSFC/SQL (do \*\*not\*\* rely on a floating VIP move in AWS). Set cluster parameters commonly used in cloud:

- `RegisterAllProvidersIP = 0`, `HostRecordTTL = 60`

- Listener name is for metadata; clients should use \*\*NLB DNS\*\* as the connect endpoint.

- Security groups: NLB → SQL SG (1433). No Internet exposure.

- Create AG replicas on AWS nodes; prefer \*\*automatic seeding\*\* (or backup/restore & join).

- Start with \*\*ASYNC\*\* commit (to avoid WAN latency on prod). After DR test, evaluate \*\*SYNC\*\* if latency allows.

- Failover mode: \*\*manual\*\* cross‑site; keep same collation/compat level. Configure readable secondaries if needed.

- Validate endpoints, log send rate, and seeding completion.

- Health checks: WSFC validation, SQL DMVs for AG state, and NLB target health.

- Planned test: manual failover to AWS, confirm app connectivity via \*\*NLB DNS\*\*, validate RPO/RTO.

- Fail back to on‑prem, confirm data parity, run integrity checks (DBCC).

- Run in parallel with \*\*ASYNC\*\* until maintenance window.

- Quiesce writes; switch to \*\*SYNC\*\*, confirm synchronized.

- Manual failover to AWS → update app connection strings (or centralize via config/Secrets Manager). Clients use \*\*NLB DNS\*\*.

- Monitor, then optionally reconfigure quorum (votes) to favor AWS as new primary site.

- Decommission on‑prem replicas when business approves.

- Keep \*\*“single‑subnet in AWS”\*\* constraint: both AWS nodes in the same subnet/AZ; use NLB to abstract primary.

- No DNN per requirement; use \*\*VNN + NLB\*\* endpoint.

- Prefer \*\*File Share Witness\*\* on‑prem for quorum until AWS becomes primary.

- Document rollback (failback) and keep backups validated.