# VPC Design for Amazon Redshift Serverless

**Purpose:** This document provides a production-ready VPC design for Amazon Redshift Serverless that meets the following requirements:

1. Use VPC, private subnets, security groups and route tables.
2. Configure security groups to restrict inbound traffic to only necessary resources.
3. Ensure Redshift Serverless is **not publicly accessible**.

## 1. High-level overview

* Single VPC dedicated to analytics (CIDR example: 10.10.0.0/16).
* Two private subnets in different Availability Zones for Redshift Serverless ENIs (minimum requirement).
* Optional public subnets for NAT gateways (if you need outbound internet for clients), but Redshift itself is placed only in private subnets.
* Interface VPC Endpoints for AWS control-plane/services (KMS, Secrets Manager, CloudWatch Logs, STS, Redshift control plane) and a Gateway Endpoint for S3.
* Tight security groups limiting ingress to only application/BIO clients or trusted CIDRs (e.g., TGW on-prem ranges).

## 2. Logical architecture (ASCII)

On-prem / Peered VPC  
 │  
 TGW / VPN  
 │  
 ┌─────────────┐  
 │ Analytics │ VPC (10.10.0.0/16)  
 └──────┬──────┘  
 │  
 Public AZ A Public Subnet A (optional: NAT) Public AZ B  
 ───────────── (10.10.0.0/24) ─────────────  
 │   
 Private AZ A Private Subnet A (10.10.10.0/24) Private AZ B  
 ───────────── - Redshift Serverless ENIs - Redshift Serverless ENIs  
 - App/BI EC2 / ECS (private) - App/BI EC2 / ECS (private)  
  
 VPC Endpoints: S3 (Gateway), KMS/Logs/SecretsManager/Redshift (Interface)  
  
 Security Groups:  
 - sg-redshift: allows 5439 from sg-app-bi OR trusted CIDRs  
 - sg-app-bi: application servers / BI tools  
 - sg-vpce: for interface endpoints (allow 443 from private CIDR)  
  
 Route Tables:  
 - Private RT: routes to S3 via gateway endpoint; 0.0.0.0/0 -> NAT (optional)  
 - Public RT: internet via IGW (for NAT/GW only)

## 3. Components and configuration details

### 3.1 VPC

* CIDR: 10.10.0.0/16 (Choose non-overlapping ranges if peered or connected to on-prem.
* Enable DNS hostnames and DNS resolution.

### 3.2 Subnets

* **Private Subnet A (AZ-1)**: 10.10.10.0/24 — use for Redshift Serverless ENIs and app clients.
* **Private Subnet B (AZ-2)**: 10.10.20.0/24 — same purpose, different AZ.
* **Public Subnet(s)** (optional): 10.10.0.0/24 / 10.10.1.0/24 — contain NAT Gateway(s) if needed.

Redshift Serverless requires at least two private subnets across different AZs to attach ENIs and allow compute placement.

### 3.3 Route tables

* **Private RT** (associated with private subnets):
  + 10.10.0.0/16 local → local
  + pl-68a54001 (S3 Gateway Endpoint) route: prefix com.amazonaws.<region>.s3 or created automatically by gateway endpoint. (For Terraform, gateway endpoint automatically adds the route associations.)
  + 0.0.0.0/0 → NAT Gateway (optional; only if clients need internet)
* **Public RT** (associated with public subnet):
  + 0.0.0.0/0 → Internet Gateway (used by NAT Gateway resources only)

### 3.4 VPC Endpoints

* **Gateway Endpoint**: S3 — keep Redshift-data-export and COPY/UNLOAD operations private.
* **Interface Endpoints** (in private subnets):
  + com.amazonaws.<region>.kms (KMS)
  + com.amazonaws.<region>.logs (CloudWatch Logs)
  + com.amazonaws.<region>.secretsmanager (Secrets Manager)
  + com.amazonaws.<region>.sts (STS)
  + com.amazonaws.<region>.redshift (Redshift control plane endpoint)

Associate endpoint security groups and allow port **443** from private CIDR or app security groups.

## 4. Security groups (Recommended concrete rules)

### Security group: sg-redshift (attached to the Redshift Serverless workgroup)

* **Type:** aws\_security\_group
* **VPC:** analytics VPC

**Ingress rules** (minimal, only what is needed): - Postgres/TCP 5439 — source: sg-app-bi (security group of application servers or BI tools) - (Optional) Postgres/TCP 5439 — source: on-prem CIDR(s) if accessing over TGW/VPN (only trusted ranges)

**Egress rules**: - All traffic (0.0.0.0/0) — or more strictly: allow to VPC endpoint IP ranges (for KMS, SecretsManager, CloudWatch) and S3 gateway (S3 gateway is handled by route table)

**Notes:** - Prefer referencing other security groups (e.g. security\_groups = [aws\_security\_group.app\_bi.id]) rather than CIDR where possible — this avoids accidental exposure when CIDRs change. - Do not open 0.0.0.0/0 for Postgres port.

### Security group: sg-app-bi (for application or BI hosts in private subnets)

**Ingress**: only from trusted sources (e.g., admin CIDRs or on-prem) **Egress**: allow to sg-redshift on port 5439, plus access to endpoints (443) as needed.

### Security group: sg-vpce (used by interface endpoints)

**Ingress**: TCP 443 from 10.10.0.0/16 (or sg-app-bi / sg-redshift whichever clients call the endpoints) **Egress**: All to allow endpoint to reach AWS services.

## 5. Redshift Serverless configuration notes

* **publicly\_accessible = false** — ensures data plane is not reachable from the public internet.
* Workgroup subnet\_ids must contain the two private subnets.
* Set enhanced\_vpc\_routing = true if you want Redshift-managed traffic to route through VPC.
* Attach the sg-redshift security group to the workgroup.
* Use a customer-managed KMS key and add an interface endpoint for KMS so key operations don’t traverse the internet.
* Use Secrets Manager (with interface endpoint) for storing DB credentials — Redshift Serverless can reference these.

## 7. Best practices & hardening

* **Least privilege** for IAM roles used by Redshift Serverless (least S3/Logs/KMS/SecretsManager permissions).
* **Restrict management access** to the VPC (bastionless model: use SSM Session Manager for EC2 administration).
* **S3 bucket policies**: limit access to the specific Redshift role or to the VPC endpoint (via aws:SourceVpce or aws:sourceVpc conditions).
* **Enable logging** (user, connection, useractivity) and ship logs to a private S3 bucket with restricted access.
* **KMS key policy**: explicitly allow the Redshift Serverless service principal and the IAM role used by the workgroup.
* **Rotate admin credentials** and use Secrets Manager.

## 8. Validation checklist (before production)

* VPC created and DNS enabled.
* Two private subnets in different AZs associated to the Redshift workgroup.
* publicly\_accessible = false on the Redshift workgroup.
* sg-redshift only allows 5439 from sg-app-bi or trusted CIDRs.
* S3 gateway endpoint exists and private route table references it.
* Interface endpoints created for KMS, Logs, Secrets Manager, STS, Redshift control plane.
* NAT Gateway only used if required; otherwise confirm no internet egress from Redshift data plane.
* CloudWatch/S3 logging enabled and verified.
* Bucket policies and KMS policies restrict access to the Redshift role and/or VPC endpoints.