OpenVPN on Fedora with Ansible — Full Guide

This README describes how to provision multi-tenant OpenVPN servers on Fedora using Ansible, with Let's Encrypt certificates (Route53), AWS NLB integration, dynamic inventory, multi-user profile management, and SSM Parameter Store publishing.

1. Prerequisites

- Ansible >= 2.14 - AWS CLI v2 configured - Collections: amazon.aws, community.aws - Fedora EC2s tagged Role=openvpn-server, Client=clienta/clientb, Environment=dev/prod - Route53 hosted zone for senthilreddy.com

2. Install Collections

Install AWS Ansible collections:

```
ansible-galaxy collection install amazon.aws community.aws
```

3. Dynamic Inventory

Configured in inventories/aws/aws_ec2.yml. Groups are role-openvpn-server, client_clienta, client_clientb, env_dev, env_prod.

```
plugin: amazon.aws.aws_ec2
regions: [ap-south-1]
filters:
  instance-state-name: running
  tag:Role: openvpn-server
keyed_groups:
  - key: tags.Role
    prefix: role
    separator: "-"
  - key: tags.Client
    prefix: client_
    separator: ""
  - key: tags.Environment
    prefix: env_
    separator:
```

4. Shared Defaults (group_vars/role-openvpn-server.yml)

Shared settings for all OpenVPN servers. Override per client as needed.

```
ovpn_proto_main: "udp"
ovpn_port_main: 1194
ovpn_enable_udp: false
ovpn_auth_mode: "mtls"
ovpn_org_name: "SRR DevOps"
ovpn_push_routes:
  - "redirect-gateway def1"
  - "dhcp-option DNS 1.1.1.1"
  - "dhcp-option DNS 1.0.0.1"
```

5. Per-Customer Vars

Example files in group_vars for each customer.

```
# group_vars/client_clienta.yml
le_domain: "vpn.clienta.senthilreddy.com"
le_email: "admin@senthilreddy.com"
ovpn_users:
  - senthilr
  - raja
ovpn_ssm_prefix: "/client-a/openvpn/clients"
ovpn_ssm_kms_key_id: "alias/ssm-sshs"
ovpn_ssm_tier: "Standard"
ovpn_ssm_param_tags:
  Project: "client-a"
  Component: "openvpn"
```

6. Provisioning

Provision all baseline OpenVPN config for ClientA.

```
ansible-playbook playbooks/site.yml -l "role-openvpn-server:&client_clienta"
```

7. Creating Client Profiles

Generate certs, render inline profiles, upload to SSM:

```
ansible-playbook playbooks/site.yml -l "role-openvpn-server:&client_clienta" --tags clients
```

8. Revoking Users

Revoke a user by adding them to ovpn_revoke_users and running revoke tag.

```
ovpn_revoke_users:
  - raja
```

```
ansible-playbook playbooks/site.yml -l "role-openvpn-server:&client_clienta" --tags revoke
```

9. Retrieving Profiles (for Users)

Profiles are pushed to SSM. Retrieve with AWS CLI:

```
aws ssm get-parameter   --name "/client-a/openvpn/clients/senthilr.ovpn"   --with-decryption   --que
```

10. Importing Profile

Import into OpenVPN client apps. On Linux:

```
sudo openvpn --config senthilr.ovpn
```

11. AWS Integration Notes

- NLB TG: TCP_UDP:1194 with HC TCP:1194 (shim included) - Route53: failover records for vpn.clientx.senthilreddy.com - IAM: route53:ChangeResourceRecordSets, ssm:PutParameter, kms:Encrypt/Decrypt if CMK used

12. User Lifecycle

- Onboarding: add username to ovpn_users, run --tags clients - Offboarding: add username to ovpn_revoke_users, run --tags revoke - Rotation: rerun --tags clients