OpenVPN on Fedora with Ansible

This guide explains how to provision OpenVPN servers on Fedora using Ansible. It supports Let's Encrypt certificates (via Route53), AWS NLB integration with a TCP health check shim, dynamic inventory via amazon.aws.aws_ec2, and multi-user client provisioning with profiles stored in AWS SSM Parameter Store.

1. Prerequisites

Make sure you have the following:

```
- Ansible installed (>=2.14)
- AWS CLI installed and configured
- amazon.aws and community.aws Ansible collections
- Fedora instances launched in ap-south-1, tagged with Role=openvpn-server
- Route53 hosted zone for senthilreddy.com with delegated control
```

2. Install Ansible Collections

Install required Ansible collections for AWS modules.

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

3. Dynamic Inventory

Dynamic inventory is already configured to use EC2 tags. Ensure your OpenVPN servers are tagged with Role=openvpn-server.

```
plugin: amazon.aws.aws_ec2
regions:
  - ap-south-1
filters:
  instance-state-name: running
  tag:Role: openvpn-server
```

4. Running the Playbook

Provision the OpenVPN servers by running the playbook:

```
ansible-playbook playbooks/site.yml -l role-openvpn-server
```

5. Creating Client Profiles

Specify client usernames in group_vars/role-openvpn-server.yml and run with the clients tag:

```
ovpn_users:
  - senthilr
  - raja

ansible-playbook playbooks/site.yml -l role-openvpn-server --tags clients
```

6. Retrieving Profiles from SSM

Profiles are uploaded to AWS SSM Parameter Store as SecureStrings. Retrieve them with AWS CLI:

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

7. Importing Profiles

Import the .ovpn file into your OpenVPN client (Windows, macOS, Linux). On Linux, run:

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

8. Revoking Users

To revoke a user certificate, set ovpn_revoke_users and run the revoke tag:

```
ovpn_revoke_users:
  - admin

ansible-playbook playbooks/site.yml -l role-openvpn-server --tags revoke
```

9. Notes

- OpenVPN runs on UDP 1194 with a TCP health shim for AWS NLB. - Firewalld automatically opens required ports. - Certificates auto-renew via Let's Encrypt DNS-01 (Route53). - Profiles are archived under /etc/openvpn/clients/clients.tar.gz on the server.