NixOS

New Host Checklist

Provisioning

- ☐ Add terraform entry for VM, then run `terraform plan`, verify, and then `terraform apply`
- ☐ Follow nixOS provisioning steps

NixOS Configuration

- ☐ Create/copy config folder for host with intended name in hosts i.e. hosts/hostname. Copy the default.nix template, and the hardware-configuration.nix file from the actual host after installation
- ☐ Add the systemd-boot bootloader config to hardware-configuration.nix for the host
- ☐ Generate SOPS/Age private key and paste to /var/lib/sops/age/keys.txt
- ☐ Generate SOPS/Age public key and paste to .sops.yaml, create separate config section
- ☐ If backups are needed for this host, create the borgmatic_pass section with local and remote subkeys, generate passwords in secrets/{hostname}.yml
  - ☐ This is the bare minimum configuration for the encrypted sops file:

```
borgmatic_pass:
  local: someStrongPassword
  remote: someOtherStrongPassword
```

Manual Steps

- ☐ If borgmatic was configured, follow these steps below
  - ☐ Add the ssh host's ssh host public key to the backup server's configuration
  - ☐ Copy the ssh host's ssh host public key to the rsyncnet authorized_keys file, then push up to rsync.net account
  - ☐ Manually run the command `borgmatic -v 2` to get the unknown ssh host prompt to appear, select yes for both

Sops-Nix Env Files

1. Create the plaintext env file to be used

   > Do not commit any plaintext env files into version control

2. Run the command to encrypt the file: `sops --input-type binary --output-type binary -e [file]`
3. To edit the file, run the following code: `sops --input-type binary --output-type binary [file]`

Sops-Nix Setup

To set up the system to run sops-nix, I usually use the host SSH key like so:

```
nix run 'nixpkgs#ssh-to-age' -- -private-key -i /etc/ssh/ssh_host_ed25519_key
```

Copy the generated private key to `/var/lib/sops/age/keys.txt` . This is the location set in the sopsFile option in `base/secrets.nix`.

No need to change from root permissions.

Afterwards, generate the public key from the private key and then copy and paste this into the .sops.yaml config file on the nix config:

```
nix shell 'nixpkgs#age' -c age-keygen -y /var/lib/sops/age/keys.txt
```

> Don't forget to run a `sops updatekeys` command if you are performing these steps after the secrets file has been created