

SOVEREIGN  
STACK





SOVEREIGN  
STACK



## Derek Smith

Presenting Sovereign Stack at  
PlebLab \_ Startup Day (/plsd)

August 22nd, 2023

tip.

tipusd.

[.farscapien.com/](https://farscapien.com/)

[/plsd](https://farscapien.com/plsd)

[/qualifications](https://farscapien.com/qualifications)

[/contact](https://farscapien.com/contact)



SOVEREIGN  
S T A C K

Sovereign Stack in a infrastructure project that enables you to **create and self-host Bitcoin-only Value4Value websites.**

[sovereign-stack.org](https://sovereign-stack.org)



# /about

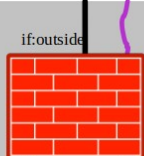
- Sovereign Stack is a complete network solution for hosting V4V websites.
- Software (mostly bash) & Website ([sovereign-stack.org](https://sovereign-stack.org))
- Started as a Ghost/BTCPay Server
  - BTCPay Server (with Core Lightning) used for BOLT11 Lightning interactions.
- **Deploys `Clams Server`** (aka ROYGBIV-stack) for BOLT12 Prism functionality.
- Deploys Ghost, Nextcloud\*, Gitea\*, Nostr Relay!
- Automates infrastructure deployments and upgrades
  - Infrastructure as code (IaC)
  - Software-defined Data Center
  - Backups, restorations, & migrations among physical cluster hosts.



Untrusted Internet  
Modem in bridge mode



Green: MGMT\_VLAN  
Blue: SERVERS\_VLAN



Trusted FW gets PUBLIC IP

if:outside  
if:mgmt  
if:servers

firewall



ss-mgmt  
System Owner



VLAN-capable  
managed switch

LXD Cluster



host-00      host-01      host-02

System Boundary

# Requirements

- Firewall (DNS, DHCP, DNSoTLS), [p]VLAN-capable switch, 1+ x64 cluster hosts capable of full VMs.
- Management Machine capable of full Vms.
- Fast & Reliable Internet with full Public IP addr
  - DOES NOT work with Carrier Grade NAT.
- SSH for remote administration of physical hosts and virtual machines.

# Users

- **System Owner / System Administrator** – the individual who downloads and executes the Sovereign Stack code; the individual risking capital in lightning channels.
- **Trusted Mobile User** – A smartphone or laptop that can VPN into a DC to access the management plane.
- **Local Website Users** – LAN/WLAN devices capable of accessing a private deployment.
- **Public Website Users** – for public deployments, untrusted devices on the public internet.

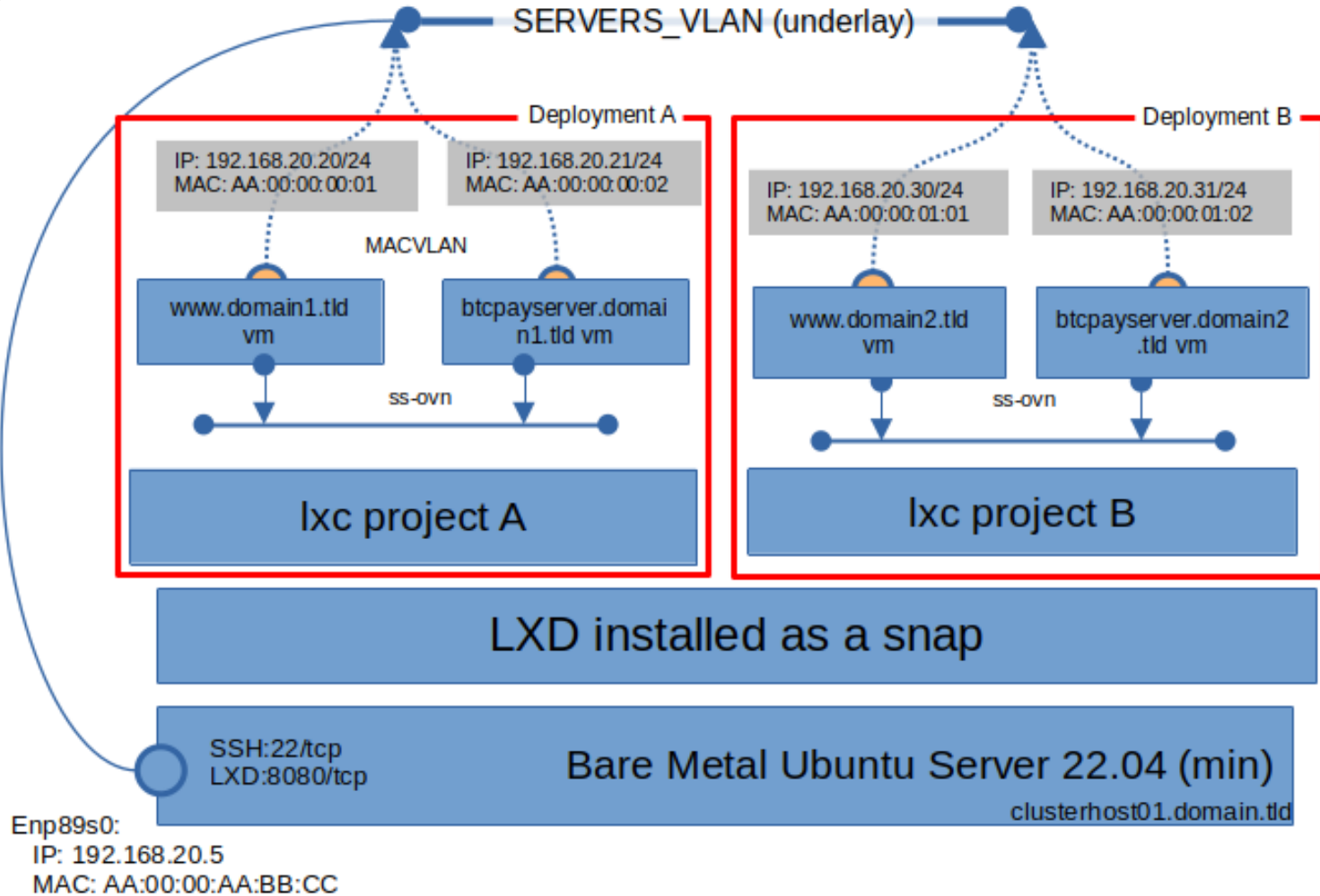


# Design Philosophy

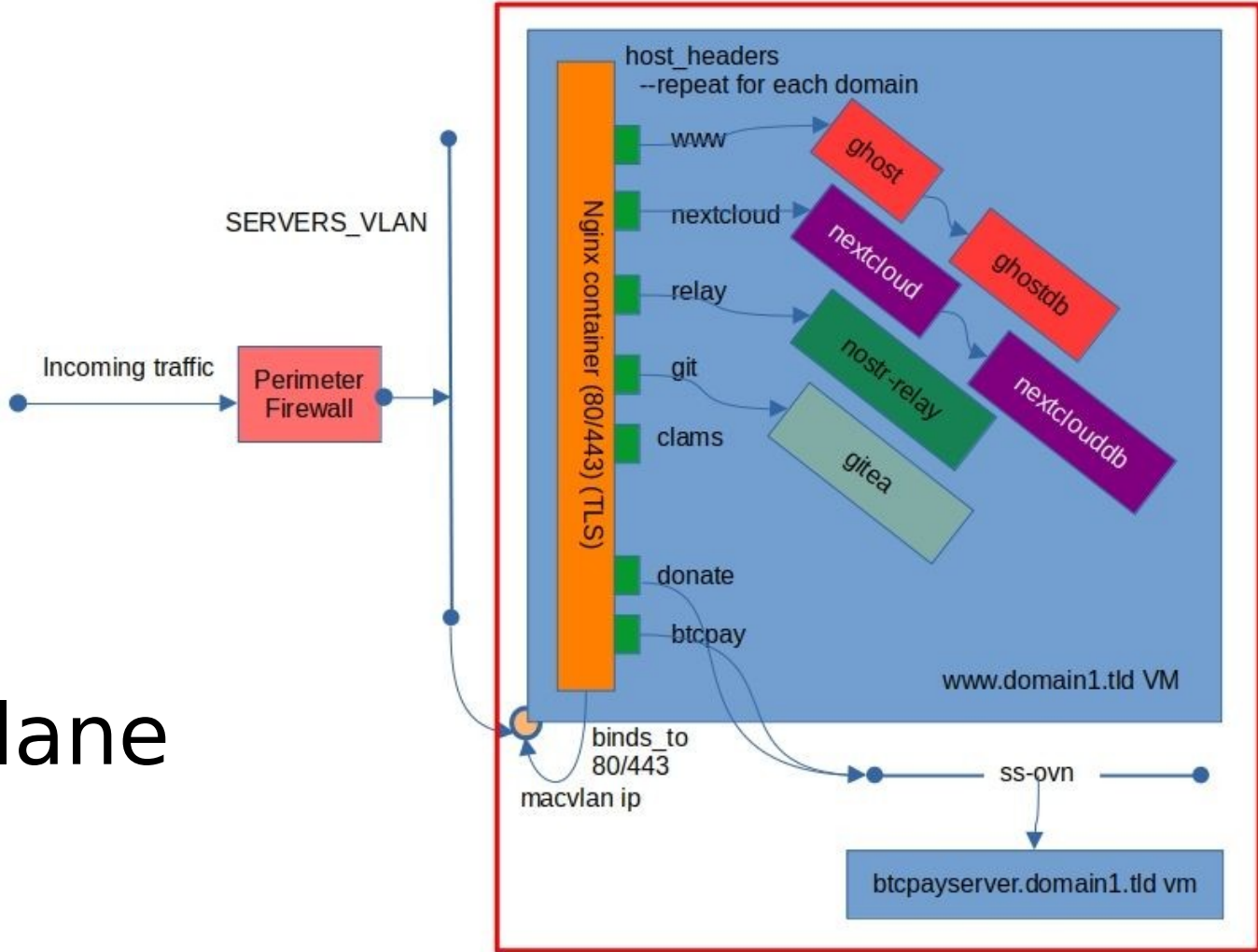
- Trust Minimization → Self-Hosting.
- Create public or intranet sites.
- Can create multiple deployments on the same hardware.
  - i.e., supports `multi-tenancy`.
- Problems to avoid:
  - Email, Public DNS\*, Exchange Rate Providers.

# Deployments

- A `Deployment` is an instantiation of a Virtual Data Center.
  - A deployment is fully contained within a LXC project.
  - Contain two full VMs connected through an OVN network bridge
  - Contains isolated VM for Clams Server.
- Each Deployment shares a base image.
- Each VM gets it's own ZFS storage volume.



# Data Plane



# Sovereign Stack – technologies

- SSH for remote administration of physical hosts and virtual machines.
- Linux System Containers (LXD) for `private-cloud`; spin up VMs and manage storage, compute, & networking.
- ZFS used for for base storage.
- All VMs are based on Ubuntu 22.04 LTS(cloud).
- Most docker images also based on Ubuntu 22.04.
- Docker API for deploying docker docker stack to remote VMs
  - Docker commands are tunneled over SSH.
  - eg., `export DOCKER\_HOST=ssh://ubuntu@www.domain.tld`

Example Value4Value  
Websites



- [oldcity-bitcoiners.info/about](http://oldcity-bitcoiners.info/about) is a Bitcoin-only meetup in St. Augustine, FL.
  - First meetup April 6th 2021.
  - Next meetup is August 31st 2023!
- Goal was to create a Lightning-only Value4Value meetup website.
- Monthly crowdfund BTC Pay widget, and donation buttons.
- The site is Bitcoin-only! No shitcoins!
- Post tags: Bitcoin & Beer, Hangout & Hack, Sponsored Events, Cancelled Events, Open Source Software, Jacksonville, Jacksonville Beach.

# satoshi-spirits.dev / about

- Satoshi Spirits is a demo website for a bar, brewery, or restaurant wanting to accept Bitcoin.
- Customers & Serving staff can both use the same interface for checkout. Order flow described in /about.
- Your website becomes your authoritative menu.
- Features a standard item cart, checkout, tipping.
- Good example of an intranet website (customers can connect to local wifi if needed).
- Other SS websites like this: moulding.money





- Sovereign-Stack.org documents the project and provides requirements/recommendations/guidance for self-hosting.
- Uses Digidocs Ghost theme, designed to be read linearly.
- Extensively documented and linked to source docs.
- Point of Sale (PoS) and Crowdfunding apps.
- Good example website for an open source project.

# farscapien.com

- A professional resume/blog, V4V enabled.
- Documents my various projects.
- Donations:
  - tipusd.farscapien.com (USD)
  - tip .farscapien.com (sats)

# roygbiv.guide

- First-of-its-kind BOLT12 Prism multi-author blog.
- Learn more with the BOLT12 Prism presentation!

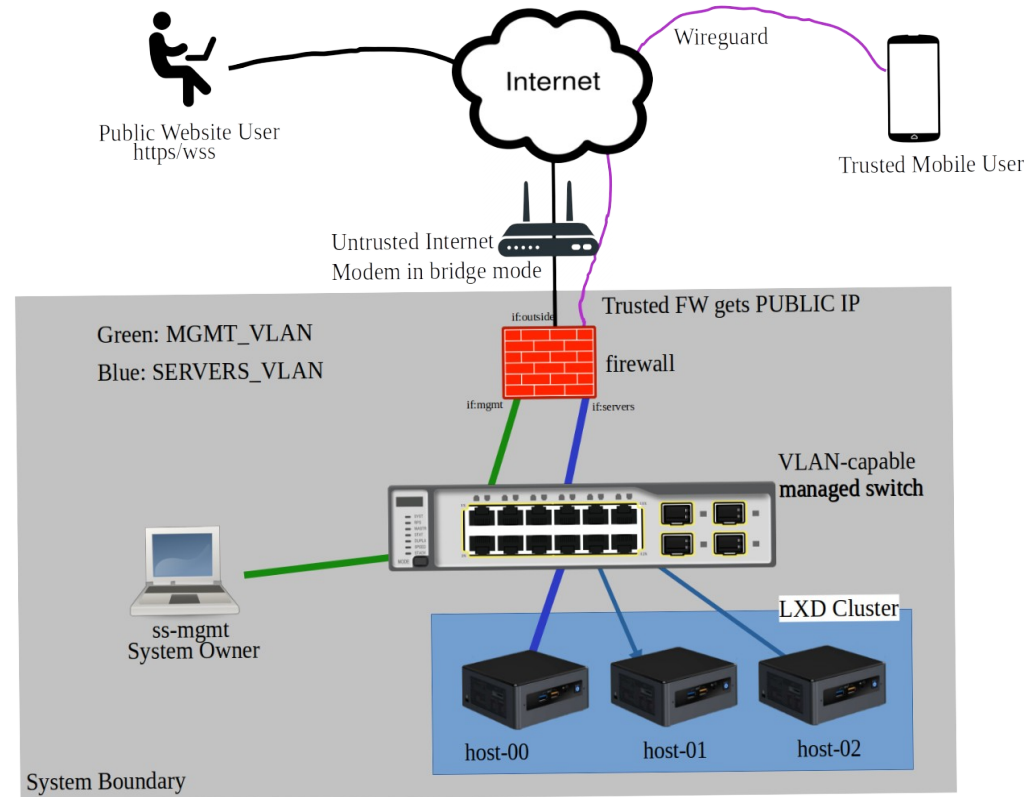
# Preparing your Network Underlay

# About Data Centers

- Availability
  - Achieve Geographic Redundancy by deploying multiple data centers.
  - Disaster Recovery – restore from backup.
  - Local High Availability\* (LXD cluster + load-balancing VIP).
- Scalability
  - Horizontal Scaling is achieved by adding additional cluster hosts to each data center.
  - You can also scale-out your data centers and distribute traffic among each data center (e.g., GeoDNS).

# Preparing your Network Underlay

- Modem in Bridge Mode
- Firewall
  - DDNS, DHCP, DNS, DNS over TLS, Wireguard
  - Traffic Policy: aliases, NAT, FW Rules



# Preparing a Cluster Host

- Get a NUC-style computer (or bigger) – x64 ONLY.
- Configure DHCP reservations & internal DNS host entries
- Install Ubuntu Server 22.04 Minimum
- Partitioning:
  - 50GB for OS
  - Partition taking the remaining space. (LXD puts a ZFS filesystem here)

# Public Website Domain Records

Type	Host	Value	Description
ALIAS	@	dc1.ddns-host.tld	This record returns the root A Record (an IP address); whatever 'dc1.ddns-host.tld' resolves to.
CAA	@	0 issue "letsencrypt.org"	Restricts certificate issuance/renewal to LetsEncrypt.
CNAME	www	domain.tld	Host record for www.domain.tld (ghost).
CNAME	btcpay	domain.tld	Host record for btcpay.domain.tld (btcpay server).
CNAME	nextcloud	domain.tld	Host record for nextcloud.domain.tld (nextcloud).
CNAME	git	domain.tld	Host record for git.domain.tld (gitea).
CNAME	relay	domain.tld	Host record for relay.domain.tld (nostr relay).
CNAME	tip	domain.tld	BTCPay Alias.



# Code Lifecycle Management

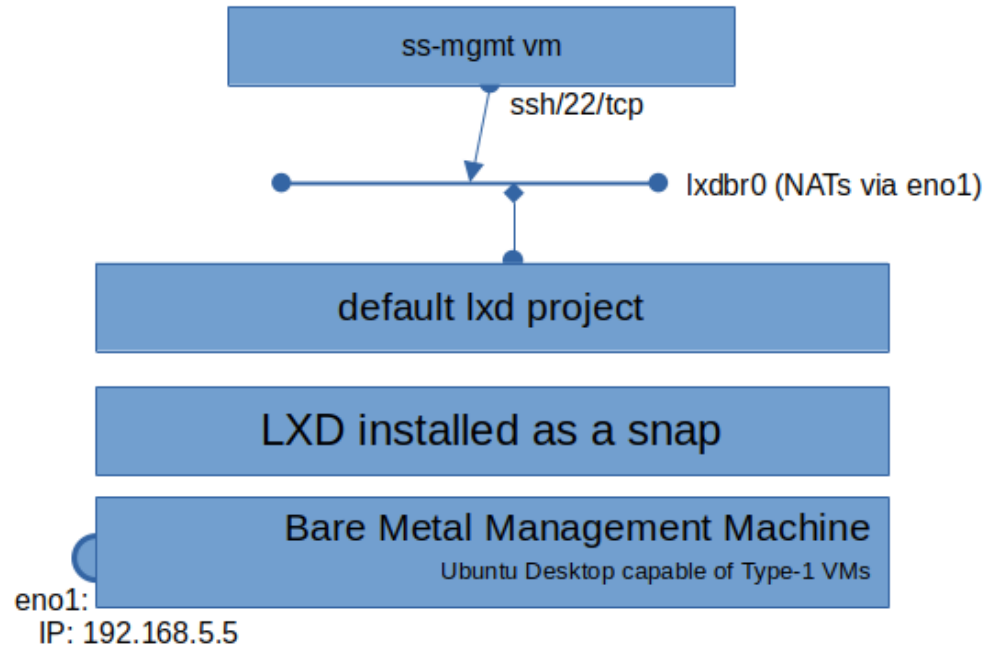
# Code Lifecycle Management

- This entire section applies to the Management Machine!
- Get the Sovereign Stack codebase:
  - `git clone --recurse submodules ~/sovereign-stack`
- Verify the code
  - Code commits are GPG signed; instructions show how to verify
- Install
  - `./install.sh`
- Update the code
- Uninstall
  - ``uninstall.sh --purge``

# Sovereign Stack Management Environment (SSME)

- The SSME is a Virtual Machine (VM) that runs on the management machine.
- Enter the SSME with the ``ss-manage`` command.
- From the SSME, you can add new remotes using ``ss-remote``, switch remotes, bring your services up and down, and other admin tasks.
- All backup archives get rsync-ed back to the SSME.

# SSME



# Command Line Interface

- **ss-manage**: enter the SSME on your management machine.
- **ss-help**: show a list of commands available to you in the SSME.
- **ss-show**: show details related to your current deployment.
- **ss-remote**: provision a remote on a cluster host.
- **ss-up**: bring your websites up according to project.conf.
- **ss-down**: take down all your websites.
- **ss-reset**: clear persistent data related to a deployment.

# ss-remote

- **ss-remote**: provision a cluster endpoint/remote.
  - After preparing a cluster host, you can run `ss-remote`
  - `ss-remote` SSHs into the cluster host and installs necessary software, i.e., LXD
  - After software is installed and configured, `ss-remote` adds LXC remote to the SSME.

# remote.conf

```
# https://www.sovereign-stack.org/ss-remote
```

```
LXD_REMOTE_PASSWORD="135kvs0e9t2k3fglkj2e09="
```

```
DEPLOYMENT_STRING="(intranet|regtest),(public|mainnet)"
```

```
REGISTRY_URL=http://docker.registry.tld:5000
```

# ss-up

- **ss-up**: bring your websites up according to `project.conf` and `site.conf` files.
  - If any `project.conf` or `site.conf` files do not exist, the script stubs them out and terminates!
  - You may need to run ``ss-up`` several times.
  - ``ss-up`` ONLY applies to your current deployment.
  - ``ss-up`` ALWAYS brings up VMs from a baseline image – i.e., immutable infrastructure.
- Several CLI options:
  - `--restore-certs`, `--restore-btcpay`, `--update-btcpay`, `--skip-wwwserver`, `--skip-btcpayserver`, `--skip-clamserver`, `--reconfigure-btcpay`, `--backup-archive-path`, `--skip-base-image`,



# project.conf<sup>1</sup>

```
# see https://www.sovereign-stack.org/ss-up/#projectconf for more info.
```

```
PRIMARY_DOMAIN="domain0.tld"
```

```
# OTHER_SITES_LIST="domain1.tld,domain2.tld,domain3.tld"
```

```
# www server
```

```
WWW_SERVER_MAC_ADDRESS=11:11:11:00:00:01
```

```
# btcpay server
```

```
BTCPAY_SERVER_MAC_ADDRESS=11:11:11:00:00:02
```

```
BTCPAY_SERVER_CPU_COUNT="4"
```

```
BTCPAY_SERVER_MEMORY_MB="4096"
```

```
# clams server
```

```
CLAMS_SERVER_MAC_ADDRESS=11:11:11:00:00:03
```

```
CLAMS_SERVER_MEMORY_MB="4096"
```

# project.conf<sup>1</sup>

```
# see https://www.sovereign-stack.org/ss-up/#projectconf for more info.
```

```
PRIMARY_DOMAIN="domain0.tld"
```

```
# OTHER_SITES_LIST="domain1.tld,domain2.tld,domain3.tld"
```

```
# www server
```

```
WWW_SERVER_MAC_ADDRESS=11:11:11:00:00:01
```

```
# btcpay server
```

```
BTCPAY_SERVER_MAC_ADDRESS=11:11:11:00:00:02
```


```
BTCPAY_SERVER_CPU_COUNT="4"
```

```
BTCPAY_SERVER_MEMORY_MB="4096"
```

```
# clams server
```

```
CLAMS_SERVER_MAC_ADDRESS=11:11:11:00:00:03
```

```
CLAMS_SERVER_MEMORY_MB="4096"
```



**DHCP Reservation  
REQUIRED for each  
VM you want to  
deploy.**

# project.conf<sup>1</sup>

```
# see https://www.sovereign-stack.org/ss-up/#projectconf for more info.
```

```
PRIMARY_DOMAIN="domain0.tld"
```

```
# OTHER_SITES_LIST="domain1.tld,domain2.tld,domain3.tld"
```

```
# www server
```

```
WWW_SERVER_MAC_ADDRESS=11:11:11:00:00:01
```

```
# btcpay server
```

```
BTCPAY_SERVER_MAC_ADDRESS=11:11:11:00:00:02
```

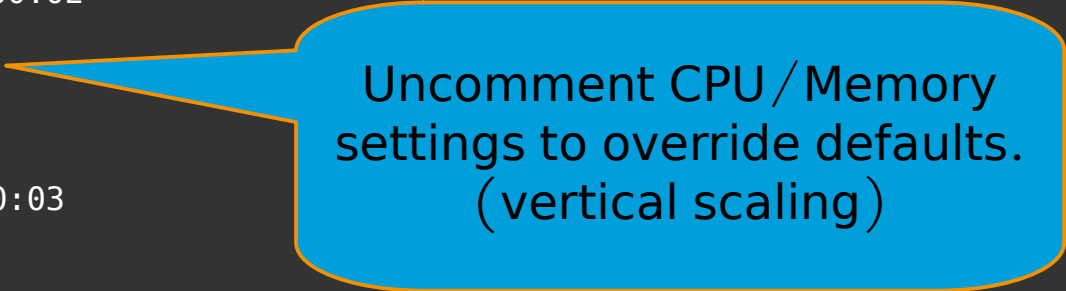
```
BTCPAY_SERVER_CPU_COUNT="4"
```

```
BTCPAY_SERVER_MEMORY_MB="2048"
```

```
# clams server
```

```
CLAMS_SERVER_MAC_ADDRESS=11:11:11:00:00:03
```

```
# CLAMS_SERVER_MEMORY_MB="4096"
```



Uncomment CPU / Memory  
settings to override defaults.  
(vertical scaling)

# project.conf<sup>1</sup>

```
# see https://www.sovereign-stack.org/ss-up/#projectconf for more info.
```

```
PRIMARY_DOMAIN="domain0.tld"
```

```
# OTHER_SITES_LIST="domain1.tld,domain2.tld,domain3.tld"
```

```
# www server
```

```
WWW_SERVER_MAC_ADDRESS=11:11:11:00:00:01
```

```
# bitcoind server
```

```
BTCPAY_SERVER_MAC_ADDRESS=11:11:11:00:00:02
```


```
BTCPAY_SERVER_CPU_COUNT="4"
```

```
BTCPAY_SERVER_MEMORY_MB="4096"
```

```
# clamd server
```

```
CLAMS_SERVER_MAC_ADDRESS=11:11:11:00:00:03
```

```
CLAMS_SERVER_MEMORY_MB="4096"
```



Create DNS entries for each VM: e.g.,  
btcpayserver.domain0.tld

# site.conf\*

```
# https://www.sovereign-stack.org/ss-deploy/#siteconf
```

```
export DOMAIN_NAME="ancapistan.io"  
export BTCPAY_ALT_NAMES="tip,store,pay,send"  
export SITE_LANGUAGE_CODES="en"  
export DEPLOY_GHOST=true  
export DEPLOY_CLAMS=true  
export DEPLOY_NEXTCLOUD=true  
export NOSTR_ACCOUNT_PUBKEY=ExampleNostrPUBKEY  
export DEPLOY_GITEA=true
```

# ss-down

- **ss-down**: brings all your services down on your current remote/project.
  - Removes all docker stacks from the VM.
  - Stops the VM, then DELETES it.
  - Add the `--purge` flag to delete any ZFS volumes associated with a VM.

# Useful Commands

- **View remotes:** ``lxc remote list``
- **Switch remote:** ``lxc remote switch <remote_name>``
- **List deployments:** ``lxc project list``
- **Switch deployment:** ``lxc project switch <project_name>``
- **List Vms in current deployment:** ``lxc list``
- **Control remote docker daemon:**
  - ``export DOCKER_HOST=ssh://ubuntu@servername.domain.tld``
- **List docker services:** ``docker service list``
- **View logs of service:** ``docker service logs <service_name>``

# Roadmap Items

- Implement continuous security assessments.
- Deprecate Nextcloud & Gitea in lieu of Nostr-alternative.
- Pre-load Blockchain/chainstate (80% complete)
- Run dockerd in rootless mode (waiting on overlay network support)
- Deploy System Containers instead of full VMs.



# Startup Ideas

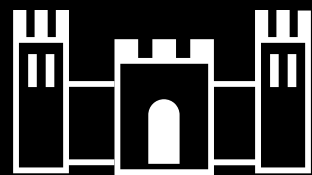
- Business Model will depends on 1) Custodial or 2) **Self-custodial**
- Individuals can deploy websites for themselves or existing businesses.
  - Onboard existing businesses onto the Bitcoin economy by creating a custom Bitcoin-only website.
  - Integrate HSM/HWW for signing for non-custodial node administration?
- A startup that helps customers create V4V websites:
  - Branding, hosting\*, monitoring, Professional Services/support, Integrations.
- Startup that creates an on-premise `datacenter-in-a-box` containing firewall, switch, cluster nodes, etc.
- ...

Want to get involved?

[sovereign-stack.org/contribute](https://sovereign-stack.org/contribute)

nostr

telegram



SOVEREIGN  
STACK

