



# NGINX for SolusVM 1.x

The new software stack for SolusVM is compatible with v1.x and will allow you to use a maintained NGINX version instead of the standard lighttpd version shipped with v1.x


 This documentation is for Master (UI) servers and Slave servers

 The following port changes have been made to UI (master) servers:

- Port 5353 has been disabled
- Port 443 is now standard and active
- Port 5656 is still active and must remain active
- Port 80 has been disabled and is only used for certificate validation

- [Installing the Repositories](#)
- [Installing the NGINX Stack](#)
- [SSL Certificate](#)
  - [Master](#)
    - [Let's Encrypt](#)
    - [Manual Setup](#)
  - [Slave](#)
- [Configuring Additional Ports](#)

## Installing the Repositories

 If `/etc/yum.repos.d/solusvm.repo` already exists it means it's already installed and you can skip this step

**SSH:**

```
yum install solusvm-release
```

## Installing the NGINX Stack

You will need to shutdown the current lighttpd service:

**SSH:**

```
service lighttpd stop  
chkconfig lighttpd off
```

Next install NGINX and the legacy configs:

### Master (UI) Server

**SSH:**

```
yum install svmstack-nginx svmstack-nginx-legacy-master-config
```

### Slave Server

**SSH:**

```
yum install svmstack-nginx svmstack-nginx-legacy-slave-config
```

Start the new service:

**SSH:**

```
service svmstack-nginx restart  
service svmstack-fpm restart
```

## SSL Certificate

### Master

#### Let's Encrypt

You can use the excellent acme.sh script as detailed here <https://github.com/Neilpang/acme.sh/wiki/Deploy-ssl-to-SolusVM>

#### Manual Setup

In most cases you will already have a valid certificate for your master which lighttpd would have been using. You can use this certificate with the new stack by copying the existing certificate to the following locations:

```
/usr/local/svmstack/nginx/ssl/ssl.crt  
/usr/local/svmstack/nginx/ssl/ssl.key
```

**/usr/local/svmstack/nginx/ssl/ssl.crt** should contain the certificate.

**/usr/local/svmstack/nginx/ssl/ssl.key** should contain the private key.



It is advised you use the default locations specified above when copying the certificates. This is an experimental feature so the configuration files may change on updates. Keeping the default locations will ensure the service continues to run and extra modules can automatically use the certificates without further intervention.

Now restart the service:

**SSH:**

```
service svmstack-nginx restart
```

### Slave

A slave can usually function on a self-signed certificate. If you require a valid certificate you can use the same process as the master certificate setup.

## Configuring Additional Ports



There is no longer a need to add additional ports. Port 443 is now standard in the new stack and the non SSL ports have been disabled, however port 5656 is still required.