Create a DNS Record

Create an A record that points your domain name to the IP address of your cloud compute instance.

Install the Required Libraries

SmokePing requires a web server, and this guide uses Nginx. SmokePing also requires Common Gateway Interface (CGI) scripting. The guide implements fcgiwrap. To install SmokePing and fcgiwrap, as well as update the server, run these commands:

```
# apt update -y

# apt dist-upgrade -y

# apt install nginx -y

# apt install fcgiwrap -y

# apt install smokeping -y
```

When prompted by the Postfix installer, choose Internet Site. When prompted for mail name, leave the name of the server. Leave the mail for postmaster and root blank.

Configure fcgiwrap

The CGI wrapper needs to interact with Nginx. Configure Nginx with the default configuration.

```
# cp /usr/share/doc/fcgiwrap/examples/nginx.conf /etc/nginx/fcgiwrap.conf
```

Configure Nginx

1. As a best practice for Nginx, delete the default web site.

```
# sudo rm /etc/nginx/sites-enabled/default
```

2. Create a no-site web site, which answers any requests destined for the host that do not contain the correct DNS name.

```
 # sudo nano /etc/nginx/sites-available/no-site
```

3. Paste the following configuration into the file.

```
server {
     listen 80 default_server deferred;
     listen [::]:80 default_server deferred;
     server_name _;

     # Return 444 (No Response)
     return 444;
 }
```

4. Save the file and exit.

5. Create a site configuration for SmokePing.

# sudo nano /etc/nginx/sites-available/smokeping

6. Paste the following configuration in the file. Change the server_name directive to match your DNS record name.

```
server {
     listen 80;
     listen [::]:80;
     server_name smokeping.example.com;

     location = /smokeping/smokeping.cgi {
             fastcgi_intercept_errors on;

             fastcgi_param   SCRIPT_FILENAME         /usr/lib/cgi-bin/smokeping.cgi;
             fastcgi_param   QUERY_STRING            $query_string;
             fastcgi_param   REQUEST_METHOD          $request_method;
             fastcgi_param   CONTENT_TYPE            $content_type;
             fastcgi_param   CONTENT_LENGTH          $content_length;
             fastcgi_param   REQUEST_URI             $request_uri;
             fastcgi_param   DOCUMENT_URI            $document_uri;
             fastcgi_param   DOCUMENT_ROOT           $document_root;
             fastcgi_param   SERVER_PROTOCOL         $server_protocol;
             fastcgi_param   GATEWAY_INTERFACE       CGI/1.1;
             fastcgi_param   SERVER_SOFTWARE         nginx/$nginx_version;
             fastcgi_param   REMOTE_ADDR             $remote_addr;
             fastcgi_param   REMOTE_PORT             $remote_port;
             fastcgi_param   SERVER_ADDR             $server_addr;
             fastcgi_param   SERVER_PORT             $server_port;
             fastcgi_param   SERVER_NAME             $server_name;
             fastcgi_param   HTTPS                   $https if_not_empty;

             fastcgi_pass unix:/var/run/fcgiwrap.socket;
```

```
    }

    location ^~ /smokeping/ {
            alias /usr/share/smokeping/www/;
            index smokeping.cgi;
            gzip off;
    }

    location / {
            return 301 http://$server_name/smokeping/smokeping.cgi;
    }
}
```

7. Save the file and exit.

8. Link the two configuration files to the Nginx configuration.

   ```
   # ln -s /etc/nginx/sites-available/smokeping /etc/nginx/sites-enabled/smokeping
   ```

# ln -s /etc/nginx/sites-available/no-site /etc/nginx/sites-enabled/no-site

9. Restart the web server.

```
# sudo service nginx restart
```

Nginx should restart without any errors. If it returns any errors, check the syntax by running:

```
# sudo nginx -t
```

10. Enable HTTPS with LetsEncrypt. Replace the example values with your DNS name and email address.

    ```
    # sudo apt install -y certbot python3-certbot-nginx
    ```

```
# sudo certbot --non-interactive --redirect --agree-tos --nginx -d smokeping.example.com -m admin@example.com
```

With this configuration completed, your web server is available with HTTPS.

6. Configure SmokePing

The final step is configuring SmokePing to use HTTPS and to ping clients.

1. Edit the General configuration

```
# sudo nano /etc/smokeping/config.d/General
```

Change the following values:

* `owner` - Set this to your name.

* `contact` - Set this to your email.

* `mailhost` - Set this to `localhost`.

* `cgiurl` - Set this to `https://smokeping.example.com/smokeping/smokeping.cgi` and change `smokeping.example.com` to your DNS record.

2. Save the file and exit.
3. Edit the Targets and add monitored hosts:

```
# sudo nano /etc/smokeping/config.d/Targets
```

4. Append the following to the end of the file (as well as any extra hosts):

```
+ websites
 menu = Website Monitoring
 title = Website Monitoring

 ++ example1
 probe = FPing
 host = one.example.com
 title = Example One

 ++ example2
 probe = FPing
 host = two.example.com
 title = Example Two
```

5. Save the file and exit.
6. Restart the SmokePing daemon.

```
# sudo service smokeping restart
```

7. Configure Postfix to use SendGrid

By default, Postfix attempts to send mail directly, which is insecure. Follow these steps to configure SendGrid as the mail relay.

Make a note of your API key, it will be shown one time.

1. Edit the main Postfix configuration file.

```
# sudo nano /etc/postfix/main.cf
```

2. Add these lines to the end.

```
smtp_sasl_auth_enable = yes
 smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
 smtp_sasl_security_options = noanonymous
 smtp_sasl_tls_security_options = noanonymous
 smtp_tls_security_level = encrypt
 header_size_limit = 4096000
 relayhost = [smtp.sendgrid.net]:587
```

3. Save the configuration.

4. Create a password file.

```
# sudo nano /etc/postfix/sasl_passwd
```

5. Add the following line. Replace API-KEY-GOES-HERE with your API key.

```
[smtp.sendgrid.net]:587 apikey:API-KEY-GOES-HERE
```

6. Save and exit the file.

7. Change the permissions, encrypt the file, and restart Postfix.

```
# sudo chmod 600 /etc/postfix/sasl_passwd

# sudo postmap /etc/postfix/sasl_passwd

# sudo systemctl restart postfix
```