

Deploying NGINX & Certificates

Introduction

We have packaged pre-configured NGINX configurations for all applications that can be deployed through Semaphore, e.g. Semaphore, NetBox, Airflow, Elastic, and so on. Within each Netos defined project in Semaphore, there will be a "SYSTEM" tab which is where you deploy NGINX and certificate settings.

Configuration

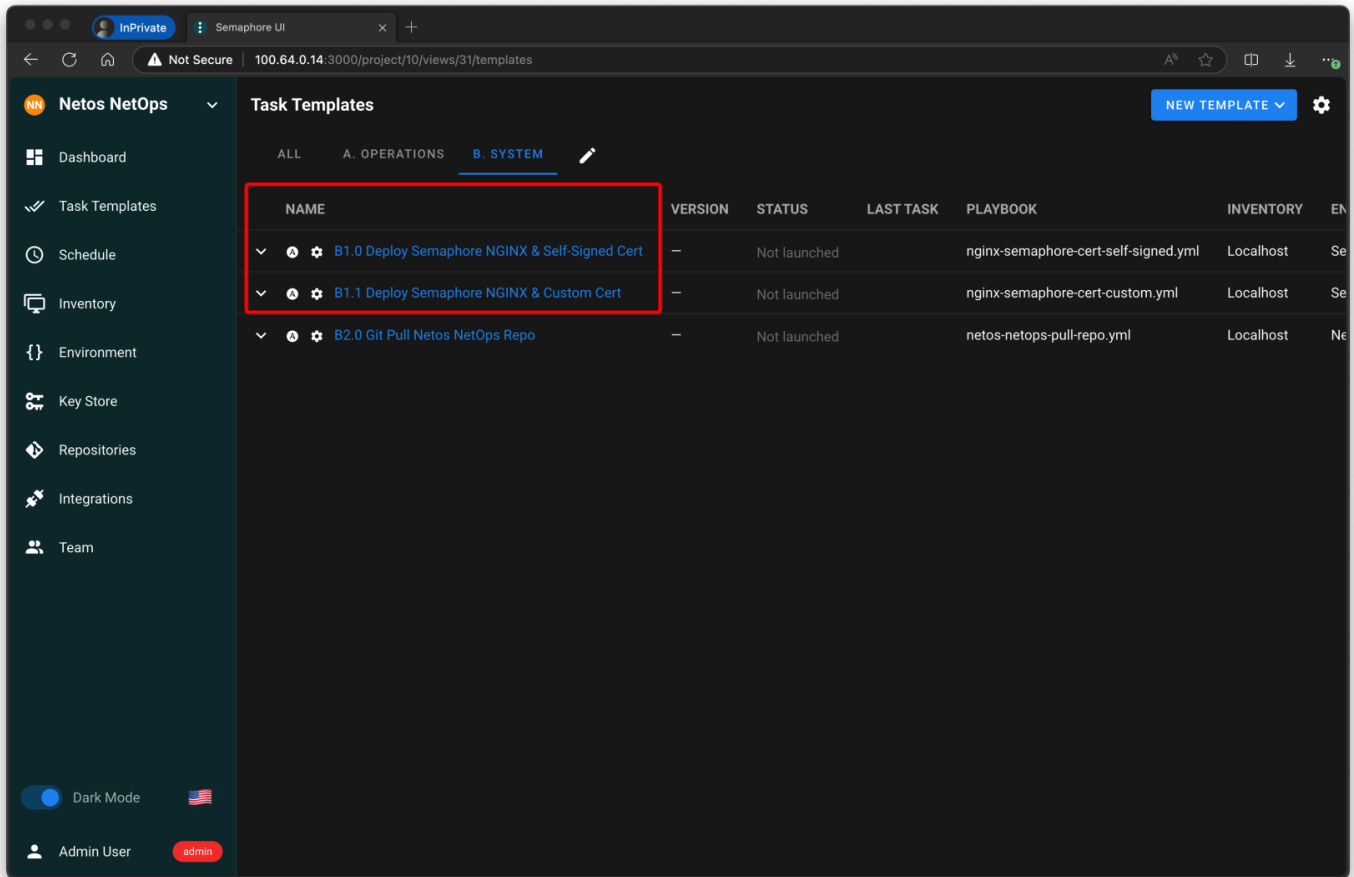
NGINX

You can find the `nginx.conf` and `{{ app_name }}.conf` files in the `nginx-*` roles in the Ansible playbooks in the Netos GitHub repositories.

We suggest using our templates because each application has different requirements, for example, Semaphore requires WSS configurations for HTMLX, and NetBox requires `/static/` to be correctly mounted. We have also configured backend keep-alives from NGINX to NetBox.

Custom vs. Self-Signed Certificates

In a lab environment a self-signed cert is ok (it'll give you a security warning when connecting via the browser). In each Semaphore project you'll see tasks like these which will provision the NGINX configuration and certificates.



Setup the Semaphore Environment

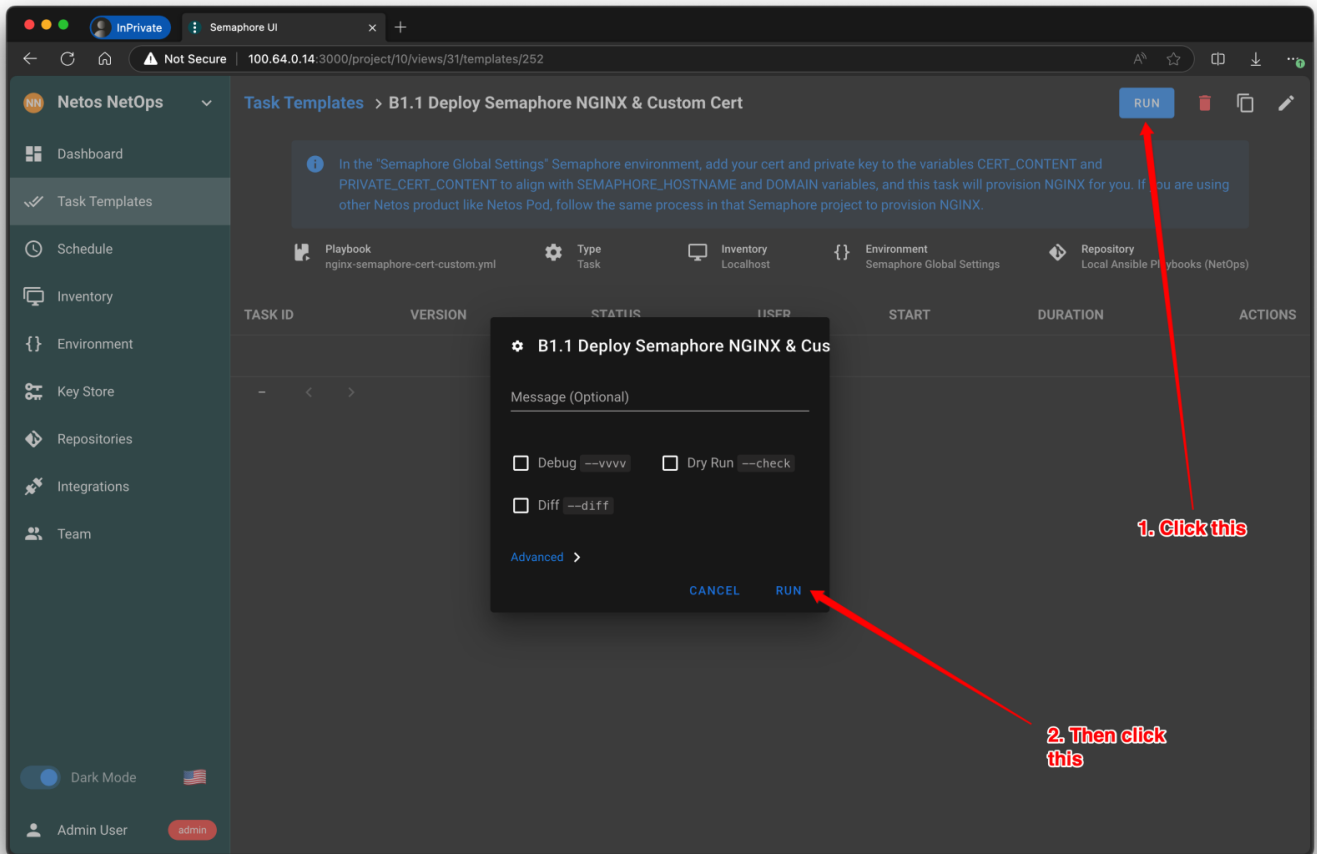
The variables are as follows. At a minimum we suggest setting the domain and hostname in ALL projects **before deploying any applications**, i.e. this example is for Netos NetOps, but you should do the same in Netos NetBox, etc.

- **DOMAIN** = e.g. `netos.io` (don't put dots or asterisk at the start)
- **SEMAPHORE_HOSTNAME** = e.g. `server01-semaphore`
- **CERT_DIR** = This is where the certs will be stored. We suggest leaving everything in `/netos/` as we have defined.
- **ORG_NAME** = e.g. Netos Networks Ltd
- **CERT_CONTENT** = the key chain for your private cert
- **PRIVATE_CERT_CONTENT** = the private cert (see example below)

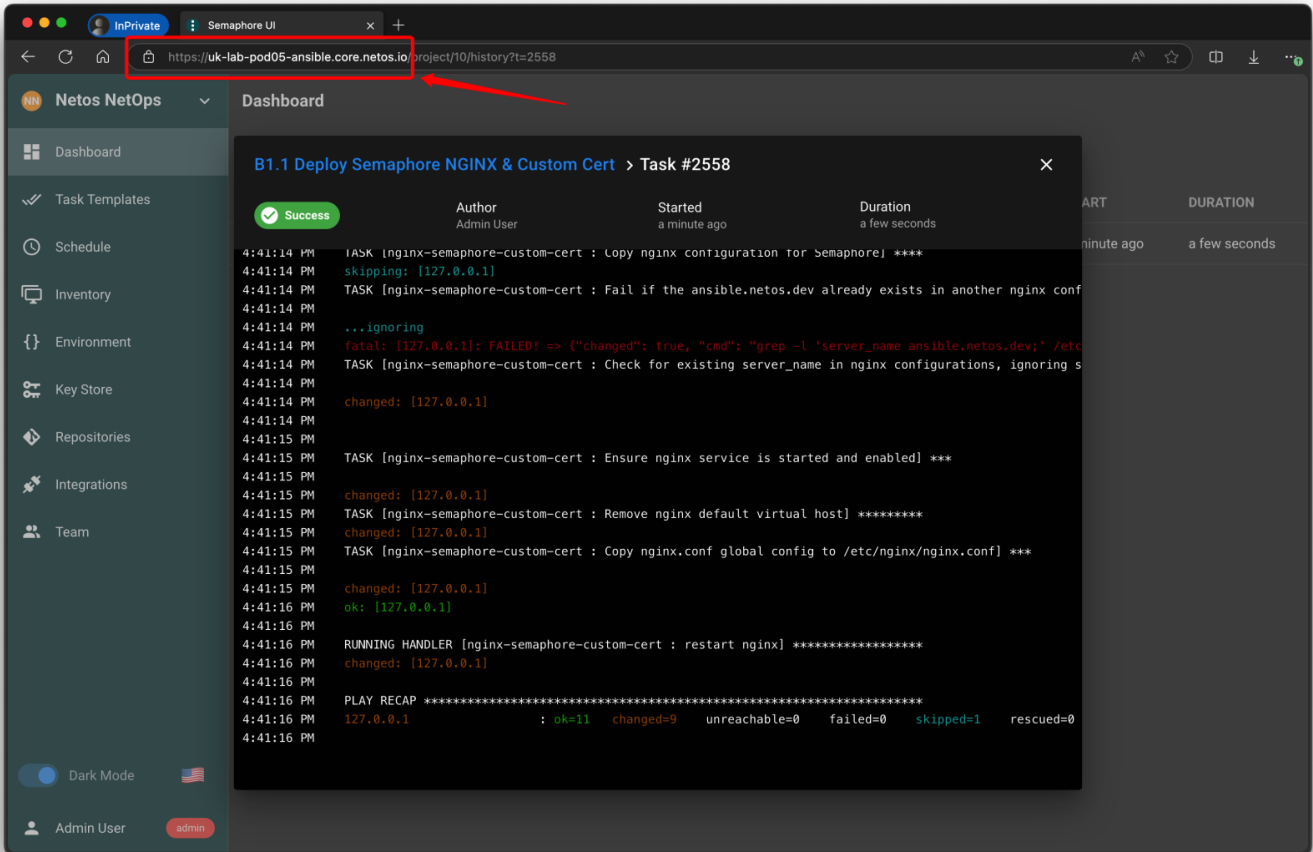

```
bTBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABDEi0b9bbErfJbPm0pIR0nA2zJKV
X2gTr1tHcBRCzMt8hjd7Fi5I66qjGV0lkg0HZyk0Z98ByU9k6FvZDxG6RCejUzBR
MB0GA1UdDgQWBBrif0qHPJ1T/pPq3c5QnU9i77NmnTafBgNVHSMEGDAWgBSePRPc
Kt+UjPnlhqFX0NvT4GLGRDANBgkqhkiG9w0BAQsFAA0CAgEAjMsdNWRtV7zxw9M7
OZ/ZwLzC+FUD87F2ghy0tFzbfP+j9PKbftmF7HJTrFv9uv2d2L6y7JnTRy0+STNY
1hcmPlbbjiFiRt9bgj5xdtXnZG2D6UG8QZVwv03AeX4YsUmo5RQx0jWxIwjlvPU
ddp9XpXg2aQsVc/ir9vPjJgCV3FXLw5Q57QCRtncFRksQ/XcdQw53bBBnMiUPzqD
h0ZSPTe/yYwa1YeeguxFos5QwtfrK7Tnlng31dSu+TljRt4LrUgTgP44egKARx
/+XX0p7xsIgFb6pAKk/JUgA4SYerH2UjRyb1D0NcB0oRFP0pe1LtI+fyRYD0iZ/b
d26w/TG0YB5b9D56PA12KEXoB0CX5tr/1zJlfSITLlRr+HpEgfX3mVfxJ6Dd5yP
9tyBYV7Z7TYPbh4D5wGR0VbVmsxVc0mub5TEfg2yLUIBG/f0pU4gfJ7p7A36G5Wd
fEp51bLxCU+yFKJLLQXeJqEd9RdTHKewgHCNrzTL54W2gF+l7udRYVDDWkTvN+p5
q5+Z23kmH2sz8cpIpRUhGRZ1lTtyokDUIHKZl+cx5IckvA4pkLzZm8eFODG1+7vH
2kPUu0me4mB8o2tLnpq2u2NcHBrcNPg4Tl5zFMvZnsXpT6n8UPMRZMtZ8i8S6GgD
NPZxatAb0Ki02SHfCquCpCqmdYMe01TIbWU=
-----END CERTIFICATE-----
```

Deploy the Certificates

In our case we have copied a wildcard full-chain cert and private key for `*.core.netos.io` into the environments in Semaphore.



After the playbook has deployed NGINX and the certs, you can change the domain in the URL and refresh the page.



Note that we configured DNS in advance of deploy NGINX and the certs. If you are running a local lab, you could set the hosts file on your workstation to point to the respective services. For example, like this:

```
10.1.1.1    uk-lab-nb05-semaphore.core.netos.io
10.1.1.1    uk-lab-nb05-netbox.core.netos.io
```

Troubleshooting

If things went wrong, you can always connect on the IP `https://x.x.x.x:3000` URL to get into Semaphore, and delete the certs and NGINX site configuration file if required.

As long as you can connect to Semaphore, you can keep running the playbook to re-apply the settings, which will replace the certs and NGINX config files.

```
netosadm@uk-lab-pod05: /etc/nginx/sites-enabled
netosadm@uk-lab-pod05:/netos/certs/semaphore$ ls -alh
total 20K
drwxr-xr-x 2 root root 4.0K Sep 22 15:44 .
drwxr-xr-x 3 root root 4.0K Sep 22 15:41 ..
-rw-r--r-- 1 root root 5.8K Sep 22 15:44 uk-lab-pod05-ansible.core.netos.io.crt
-rw----- 1 root root 1.7K Sep 22 15:44 uk-lab-pod05-ansible.core.netos.io-private.key
netosadm@uk-lab-pod05:/netos/certs/semaphore$ cd /etc/nginx/sites-enabled/
netosadm@uk-lab-pod05:/etc/nginx/sites-enabled$ ls -alh
total 12K
drwxr-xr-x 2 root root 4.0K Sep 22 15:44 .
drwxr-xr-x 8 root root 4.0K Sep 22 15:41 ..
-rw-r--r-- 1 root root 1.5K Sep 22 15:44 semaphore.conf
netosadm@uk-lab-pod05:/etc/nginx/sites-enabled$
netosadm@uk-lab-pod05:/etc/nginx/sites-enabled$
netosadm@uk-lab-pod05:/etc/nginx/sites-enabled$
```

Then restart the NGINX process once the above files are deleted: `sudo systemctl restart nginx`.

Revision #8

Created 2024-09-22 11:59:17 UTC by Richard Foster

Updated 2024-10-09 13:30:50 UTC by Richard Foster