

DEV Team Infrastructure Home	2
DEV Team Supporting Infrastructure	3
DEV Infrastructure	4
STAGING Infrastructure	5
QA Infrastructure	6
PRODUCTION Infrastructures	7
DEV Team Service map	8
DEV Services	10
STAGING Services	11
QA Services	12
PRODUCTION Services	14
External Dependencies - Services used	15
DEV Dependencies	16
Services Infra Dependencies	17
Hardware Dependencies	18
INFRA Services	19
Misc. Procedures for our internal INFRA	20
All Passwords	21
Dev Team account for general emails	22
Hardware/OS specifics info to work at NovAliX	23
Tips for Ubuntu users	25
Access NASSYN from Ubuntu	26
Install Novalix VPN on ubuntu 22.04	28
AnyDesk Windows to Ubuntu	30
CI/CD Process	31
Installation logs for builder and server	34
Proxy and Nginx configuration	38



DEV Team Infrastructure Home

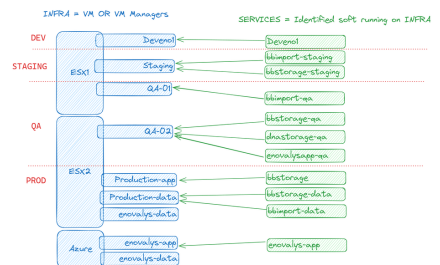
Everything that is **not directly development** but is used to **support development, deployment and the developer day-to-day work**.

Find the list of all of the machines we are using (our **infrastructure**) : [DEV Team Supporting Infrastructure](#)

Find the list of all the services we are developing (our **service mesh**) : [DEV Team Service Map](#)

i A new line in **Service Map** MUST reference a line in **Supporting Infrastructure** because a service is installed in/on a piece of infrastructure.

Example of relations between INFRA and SERVICES



Find our procedure and **other knowledge** about **where and how your code will run** at NovAliX, what computer, laptops, software, you'll be using.

👉 This space has a strong link with the IT Infra Team.

We love ❤️ them and must include them in all of our extra work that impact or require the infrastructure expertise.

DEV Team Supporting Infrastructure

What is it

List of the Infrastructure available to develop / test / deploy our apps and services.

It describes where are located the machines and how to access them.

It **doesn't** describe how to consume the service and what services are deployed on it.

Data

(☐ = internal DNS only, not public)

DEV Infrastructure

Adress	Access	Name	Where	DNS
192.168.90.16	rdp:3389 / ssh	deveno1	SXB-Aquila	☐ deveno1.novalix.com
192.168.90.17	rdp:3389	deveno2	SXB-Aquila	☐ deveno2.novalix.com
192.168.90.235	ssh	DevAnsible	???	☐ ansible.novalix.com
192.168.90.233	ssh	Github Actions Runner 01	???	☐ github-actions-runner-01.novalix.com
192.168.90.234	ssh	Github Actions Runner 02	???	☐ github-actions-runner-02.novalix.com

(☐ = internal DNS only, not public)

STAGING Infrastructure

addr	access	name	Where	DNS
192.168.90.121	ssh	integration-lin (NX-SXB-INTEGRATION)	SXB-Aquila	☐ staging-01.novalix.com
192.168.90.162	ssh	enovalysapp-staging	SXB-Aquarius	☐ enovalysapp-staging.novalix.com
192.168.90.163	ssh	enovalysdata-staging	SXB-Aquarius	☐ enovalysdata-staging.novalix.com

(☐ = internal DNS only, not public)

QA Infrastructure

(☐ = internal DNS only, not public)addr	access	name	Where	DNS
51.13.94.185	rdp:3389	integration-services / recette	Azure Novalix VM	recettage- win.novalix.com
192.168.90.120	ssh	integration-ubuntu-01	SXB-Aquila	☐ qa-01.novalix.com
192.168.90.160	ssh	enovalys-integ-APP	SXB-Aquila	☐ enovalysapp.novalix.com
192.168.90.161	ssh	enovalys-integ-DATA	SXB-Aquila	☐ enovalysdata.novalix.com

(☐ = internal DNS only, not public)

PRODUCTION Infrastructures

addr	access	name	Where	DNS
20.4.22.23	rdp:53148	production-APP-BACKUP	Azure Novalix VM	gw.soft-enovalys.com
/	azure CLI rdp	production-APP-Atheo	Azure Atheo VM	gw.soft-enovalys.com
40.115.59.236	rdp:51134	production-DATA 2008	Azure Novalix VM	enovalysdata.cloudapp.net
104.45.49.27	rdp:3389	production-DATA 2019	Azure Novalix VM	enovalysdata2019.westeurope.cloudapp.azure.com
/	azure CLI rdp	production-DATA-Athéo	Azure Atheo VM	in local network with production-APP-Atheo
168.63.107.116	rdp:3389	production-services (win)	Azure Novalix VM	services.novalix.com
168.63.64.211	ssh	production-ubuntu ???	Azure Novalix VM	production.novalix.com ???
WIP	ssh	WIP	WIP	☐ prod-app-01.novalix.com
WIP	ssh	WIP	WIP	☐ prod-data-01.novalix.com
192.168.90.22	ssh	Intranova	???	☐ intranet.novalix.com
192.168.128.101	ssh	delcalculation2	Server at Illkrich Bat B	☐ delcalculation2.novalix.local
192.168.128.212	rdp:3389	DEL-APP	???	???

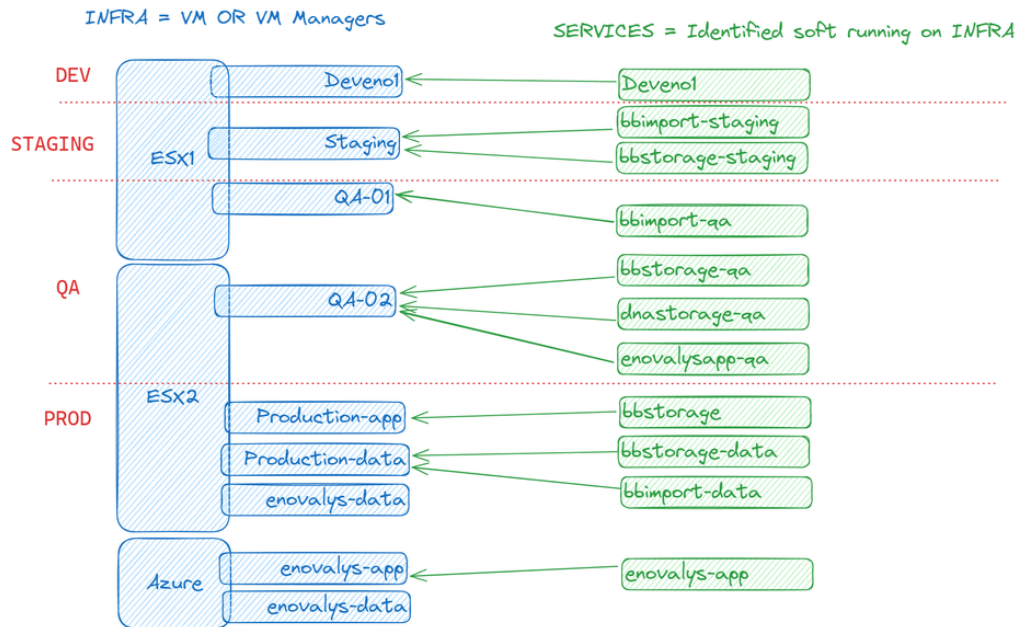
(☐ = internal DNS only, not public)

DEV Team Service map

What is it

- List of the services available for user consumption or other services consumption.
- It describes how to consume the service, **not what's the hardware or precise location**

Example of relations between INFRA and SERVICES



Rules

- The column "Where" in [DEV Team Service map](#) should have the name of a location in [DEV Team Supporting Infrastructure](#)
- □ = internal DNS only, not public

Meaning :

- **DEV** : Used for or ongoing development and are instable
- **STAGING**: Tested for deployment and integration with other deployed services
- **QA** : Available for testers and beta users to use, similar to production, isn't impacted by deployment tests
- **PRODUCTION** : Available for production, sensible data, only code that's been through all the previous envs can be put here.

XMind prototype version:

The goal of this file is to map the service mesh of every production services at NovAliX



Network Error

An error occurred, please try again. If the problem persists, please contact the support team.

[Contact Support](#)

DEV Services

i A new line in **Service Map** MUST reference a line in **Supporting Infrastructure** because a service is installed in/on a piece of infrastructure.

ServiceName	Where (infra)	Usage Port	Usage Dns	Service Manager	Installation Comment
Enovalys Dev Env Alex	deveno1	80	☐ deveno1.novalix.com	aweisser	VS Studio 2013 + SQL Management
Enovalys + DELTA Dev Env Frank	deveno2	80	☐ deveno2.novalix.com	fhoonakker	VS Studio 2013 + SQL Management + VS Studio 2022 for DELTA

STAGING Services

i A new line in **Service Map** MUST reference a line in **Supporting Infrastructure** because a service is installed in/on a piece of infrastructure.

ServiceName	Where (infra)	Usage Port	Usage Dns	Service Manager	Installation Comment
eNovalys Back + Silverlight	enovalysapp-staging	80	enovalysapp-staging.novalix.com	fhoonakker / aweisser	Win Server 2019
eNovalys flask services	enovalysapp-staging	80->6767	flask-staging.novalix.com	fhoonakker	Win Server 2012, Flask on IIS , host lots of unsecured small services
eNovalys Marvin	enovalysapp-staging	80->8080	marvin-staging.novalix.com	fhoonakker / aweisser	Win Server 2019
eNovalys Next App	enovalysapp-staging	80	next-staging.novalix.com	fhoonakker / aweisser	C:/WebSites/next
eNovalys SQL Server	enovalysdata-staging	80	enovalysdata-staging.novalix.com	fhoonakker / aweisser	
AnalyticSync CRON TASK	integration-lin	no-port exposed	no-url	fhoonakker / aweisser	Consume the anyalitycal nassyn \\nx-sxb-file01.novalix.local with a cron task, no exposed service in /docker_apps/analyti_sync
BBsStorage	bbsstorage-staging		bbsstorage-staging.novalix.com	clumineau / gdoignon	

QA Services

i A new line in **Service Map** **MUST** reference a line in **Supporting Infrastructure** because a service is installed in/on a piece of infrastructure.

ServiceName	Where (infra)	Usage Port	Usage Dns	Service Manager	Installation Comment
CALIX API	integration-ubuntu-01	80->4789	api-calix-recettage.novalix.com	cburkhart	docker -> /docker_apps/calix
CALIX front	integration-ubuntu-01	80	calix-recettage.novalix.com	cburkhart	/var/www/calix
BBs Import API	integration-ubuntu-01	80->4455	api-bbsimport-recettage.novalix.com	ddamato	docker -> /docker_apps/bbsimport
BBs Import Front	integration-ubuntu-01	80	bbsimport-recettage.novalix.com	ddamato	/var/www/bbsimport
BBsStorage API	integration-ubuntu-01	80->5959	api-bbsstorage-recettage.novalix.com	gdoignon/clumineau	docker → /docker_apps/bbsstorage
BBsStorage front	integration-ubuntu-01	80	bbsstorage-recettage.novalix.com	gdoignon/clumineau	/var/www/bbsstorage
BBId Gen	integration-ubuntu-01	80->6987	api-bbidgen-recettage.novalix.com	ddamato	docker -> /docker_apps/nsn_generator
BBId Generator front	integration-ubuntu-01	80	bbidgen-recettage.novalix.com	ddamato	/var/www/bbidgen
NovaTrack front	integration-ubuntu-01	80	novatrack-recettage.novalix.com	lgoarant	/var/www/novatrack
NovaTrack API	integration-ubuntu-01	80->5784	api-novatrack-recettage.novalix.com	lgoarant	docker -> /docker_apps/novatrack
RDKit service API	integration-ubuntu-01	80->6667	rdkit-recettage.novalix.com	aweisser	docker -> /docker_apps/RDkit-service

eNovalys Back + Silverlight	enovalys-integ-APP	80	□ integration.novalix.com / □ enovalysapp.novalix.com	fhoonakker / aweisser	Win Server 2019
eNovalys flask services	enovalys-integ-APP	80->6767	□ flask-integration.novalix.com	fhoonakker	Win Server 2012, Flask on IIS , host lots of unsecured small services
eNovalys Marvin	enovalys-integ-APP	80->8080	□ marvin-integration.novalix.com	fhoonakker / aweisser	Win Server 2019
eNovalys Next App	enovalys-integ-APP	80	□ next-integration.novalix.com	fhoonakker / aweisser	C:/WebSites/next
eNovalys SQL Server	enovalys-integ-DATA	80	□ enovalysdata.novalix.com	fhoonakker / aweisser	

PRODUCTION Services

i A new line in **Service Map** MUST reference a line in **Supporting Infrastructure** because a service is installed in/on a piece of infrastructure.

ServiceName	Where (infra)	Usage Port	Usage Dns	Service Manager	Installation Comment
eNovalys backup	production-APP-BACKUP	80	soft-enovalys.com	aweisser	old version with silverlight in the mean time that athéo is ready
eNovalys flask services	production-APP-BACKUP	80->6767	flask.soft-enovalys.com	fhoonakker	Win Server 2012, Flask on IIS , host lots of unsecured small services
eNovalys Marvin	production-APP-BACKUP	80->8080	marvin.soft-enovalys.com	fhoonakker / aweisser	Win Server 2012
eNovalys Next App	production-APP-BACKUP	80	next.soft-enovalys.com	fhoonakker / aweisser	Win Server 2012, C:/WebSites/next
eNovalys Beta App	production-APP-BACKUP	80	beta.soft-enovalys.com	fhoonakker / aweisser	Win Server 2012, C:/WebSites/beta
Deveveloper Identity	production-APP-BACKUP	80	devs.novalix.com	aweisser	Win Server 2012, C:/WebSites/devs.novalix.com
eNovalys GRoS	production-APP-Atheo	80	/	aweisser / athéo	New backed up and secured infra , not ready
eNovalys SQL Server 2019	production-DATA-Athéo	?	/	athéo / aweisser	inside local network , not publicly accessible
eNovalys SQL Server 2019	production-DATA	?	enovalysdata2019.westeurope.cloudapp.azure.com		currently used
molecule-crawler	production-services	80->6767	crawler.novalix.com	cburkhart	Flask on IIS
docker image registry (WIP)	production-services	80	docker.novalix.com	aweisser	Docker with WSL hosting the official registry server image
INTRANOVA	intranova	80	intranet.novalix.com		

External Dependencies - Services used

What is it

List of all the external services we used to work on a daily basis.

DEV Dependencies

Where	What / who	Contact / Admin
Structure operations in backend	Chemaxon Libraries / apache java module	fhoonaker
Structure operations in front-end	Chemaxon App MarvinJS	fhoonaker
DB DEV	ZenConseil	ZenConseil
Backend DEV	JC-Chalte	jcchalte
Frontend DEV	aweisser / lgoarant	aweisser / lgoarant
Labbook DEV	fhoonaker / lgoarant	fhoonaker / lgoarant
WebCrawler Service	Microservice	cburkhart

Services Infra Dependencies

Where	What / who	Contact / Admin
Novalix Team mails	devs@novalix.com	aweisser / fhoonakker
Mail batch with templates	Mailchimp	devs@novalix.com
DNS Service	namebay	fhoonaker / aweisser / dlecoustrour
Novalix Local DNS	adbatb dnsmgmt.msc	dlecoustrour / jhermann
Recettage Nginx proxy manager	recettage-lin.novalix.com	aweisser / devs@novalix.com
Integration Nginx proxy manager	integration-lin.novalix.com	aweisser / devs@novalix.com
SSL Service	namebay	fhoonaker / sgarrigue
Bug reporting	Jira Software	fhoonaker / aweisser / devs@novalix.com
Wiki / FAQ / other doc	Jira Confluence	fhoonaker / aweisser / devs@novalix.com

Hardware Dependencies

Where	What / who	Contact / Admin
DEV IaaS	Internal VMWare Server ESX-DEV-01	dlecoustrou / jhermann
INTEG IaaS	Internal VMWare Server SXB-Aquila	dlecoustrou / jhermann
PROD IaaS	Microsoft Azure	fhoonaker / aweisser
Infra details lookup	LanSweeper	sgarrigue / dbadique / dlecoustrou
NAS	nassyn on 192.168.90.200	dlecoustrou

INFRA Services

addr	access	name	dns
192.168.90.45	http:80	Hyperviseur ESX-INTEG-01	▯sxb-aquila.novalix.local
192.168.90.52	http:81, login = AD UserID+pswd	LanSweeper, infra search and lookup	
192.168.0.210	dns	▯ADBATB.novalix.local	adbatb / ▯adbatb.novalix.local

Misc. Procedures for our internal INFRA

All Passwords

- Have **KeePassXC** installed ([Procédure d'utilisation KeePassXC](#))
- Have access to the `\\K:` (ask IT if not)
- Go to the file : `\\K:\Departements\IT\Mots de passe.kdbx`
- Input the password (Ask Team member or IT if you don't have it)
- Tada ✨

If you're on linux : [Access NASSYN from Ubuntu](#)

Dev Team account for general emails

Emails on the DEV team's behalf

Be sure to use a general email when you need to communicate information with a specific generic account (like a user with specific rights for accessing some folder during an import)

When doing so, **register the newly created account in the keypass in “DEV Team/Comptes partagés”** and explain what's the use of this account.

We have one accounts that is used for general purpose in the name of the dev team which is :


devs@novalix.com

Email service in your app

You can use it to send mails for your application to your users with the following configuration :

```
1 smtp_server = "smtp.office365.com"
2 smtp_port = 587
3 smtp_login = "devs@novalix.com"
4 smtp_password = <YOURPASSWORD>
```

cf. [All Passwords](#)

 Limitations : There is a quota of parallel mails send.

Be sure to make you email service able to retry failed emails and send grouped emails in a controlled, timed, queue.

Hardware/OS specifics info to work at NovAliX

You can install anything you like that will increase your development confort, but it's also nice to work on a common set of tools.

So we recommend using those tools, which we have a license for :

Software requirements

last updated (Jan. 2023)

Necessary :

- [JetBrains Rider](#)
- [JetBrains Pycharm](#)
- [JetBrains DataGrip](#)
- [Docker Desktop \(Win\) / Docker \(Linux\)](#) (containerisation, necessary for deployment)
- [Postman](#) (API testing)
- [KeePassXC](#) (password keeper)

Nice to have :


- [Rambox](#) (Linux, email client)
- [Visual Studio Code](#) (powerful and quick IDE for fast stuff)
- [Teams](#)
- [Outlook](#)
- [GitExtension](#)
- [Meld](#) (diff checker, native to other IDE)

Libraries and Frameworks :

- [Python3](#)
- [miniconda](#)
- [NodeJS](#)
- [NPM](#)

Service rights

You'll need rights to those services. If you don't have them, ask your team lead :

What	Who to contact
Personal Github Account	You
JetBrain Licences	Frank
Pre-prod accounts	Alex
 Rights on specific projects	Alex
[Azure DevOps] access for your NovAliX AD Account	Alex
[Jira Software] access accounts	Alex

[Jira Confluence] access accounts	Alex
VPN Access & token	IT INFRA

Hardware equivalent requirements

last updated (Jan. 2023)

- 1 AMD Ryzen Pro 5850U 8core
- 2 32Go RAM
- 3 1To SSD
- 4

Tips for Ubuntu users

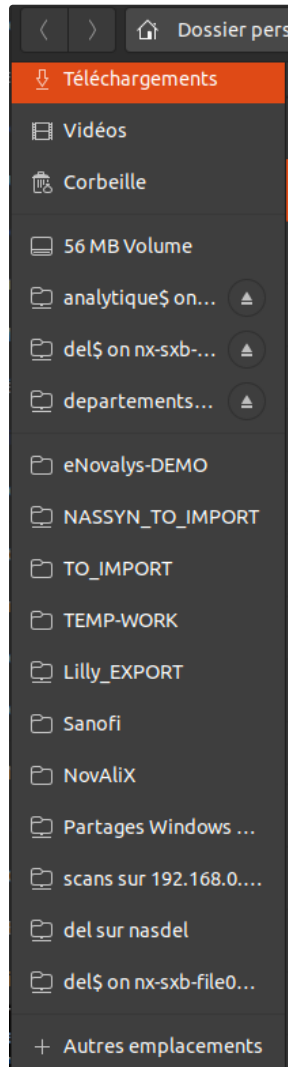
Last updated	OS	Commentary
Jan. 2023	Ubuntu 22 LTS	Lenovo with Lenovo Dock GEN2 will work in dual screen but not Dock USB C hybrid.
Jan. 2023	Ubuntu 22 LTS	KeepassXC Needed for Ubuntu, not KeepassX
Jan. 2023	Ubuntu 22 LTS	Teams: you should install teams from the Microsoft website: Télécharger les applications de bureau et mobiles Microsoft Teams Microsoft Teams , download the last Linux version and install it with the command <code>sudo dpkg -i file.deb</code> then be sure to start your desktop with Xorg and not Wayland; look here: Comment Basculer Entre Wayland Et Xorg Dans Ubuntu - Tech Tribune France

Access NASSYN from Ubuntu

Related : [All Passwords](#)

Access the nassyn

1. Just open “nautilus” (ubuntu file browser) and click on “Other place” on the bottom left of the browser:



2. Enter the following path:

```
1 smb://nx-sxb-file01.novalix.local/
```

3. Click on “connect” and enter your credentials. The domain should be “novalix.local”.

4. You should have access to the nassyn.

5. You can create shortcut to ease the access to some folders.

i Note that you may not have the right to access all the folders. If you are supposed to access it and it not the case, open a ticket here: <https://novalix.atlassian.net/servicedesk/customer/portals> section IT Helpdesk.

Access password files

From Linux to access the password file, you will follow the following general process:

1. download the password file from the NAS
2. open it with the password
3. [Optionally] update the file and upload it to the NAS.

Find below some scripts and details to help you.

Download the password file

Use the following script:

```
1 cd ~
2 rm -rf Mots-de-passe.kdbx
3 smbclient //nx-sxb-file01.novalix.local/Departements$ -U fhoonakker -W novalix -c "get \"IT\Mots de passe.kdbx\""
4 keepassxc Mots-de-passe.kdbx
```

Replace **fhoonakker** by your own NovAliX username.

The script will ask you your NovAliX password to download the file.

Then you will need the password for the file. Ask someone in the team to provide you this password.


Upload the password file once modified

 If you need to add a new password, you will need to **follow this process (this is mandatory to not lose any data)**:

1. Download the last version of the file (see above)
2. Modify the file
3. Immediately upload it with the following script:

```
1 cd ~
2 smbclient //nx-sxb-file01.novalix.local/Departements$ -U fhoonakker -W novalix -c "put Mots-de-passe.kdbx \"IT\Mo
```

Replace **fhoonakker** by your own NovAliX username.

 **Be aware that if someone has modified the password at the same time as you, we may lose one of the modification. This is the limitation of this method, that's why we need to be quick.**

Install Novalix VPN on ubuntu 22.04

Install/downgrade openVPN into ubuntu 22.04

1. Uninstall the current OpenVPN version if installed:

```
sudo apt remove openvpn
```

2. Install libssl1.1 binary

- Go to [1.1.1f-1ubuntu2.12 : libssl1.1 : amd64 : Focal \(20.04\) : Ubuntu](#)
- download the `libssl1.1_1.1.1f-1ubuntu2.12_amd64.deb` file in the **Downloadable files** section.
- Double-click on the file and open it with Software Install (GUI)

3. Install OpenVPN 2.4.7

- Go to [2.4.7-1ubuntu2.20.04.4 : openvpn : amd64 : Focal \(20.04\) : Ubuntu](#)
- Download the `openvpn_2.4.7-1ubuntu2.20.04.4_amd64.deb` file in the **Downloadable files** section
- Double-click on the file and open it with Software Install (GUI)

4. (Re)-install NetworkManager OpenVPN GUI: `sudo apt install network-manager-openvpn-gnome network-manager-openvpn`

5. Block the automatic update of openvpn `sudo apt-mark hold openvpn libssl1.1 network-manager-openvpn network-manager-openvpn-gnome`

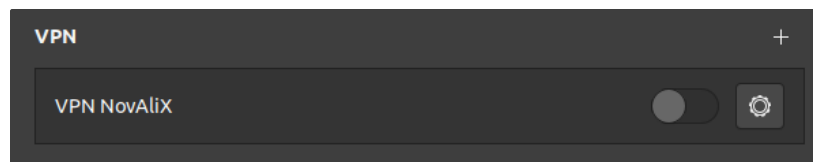
Please note that steps 1 and 5 should be run as a command in the terminal. This requires you to have appropriate permissions and know your local machine's username and password.

Additionally, for steps 2 and 3, after downloading the .deb packages, you can double-click them in Nautilus/file manager and select "Software Install" as a required option to open the package.

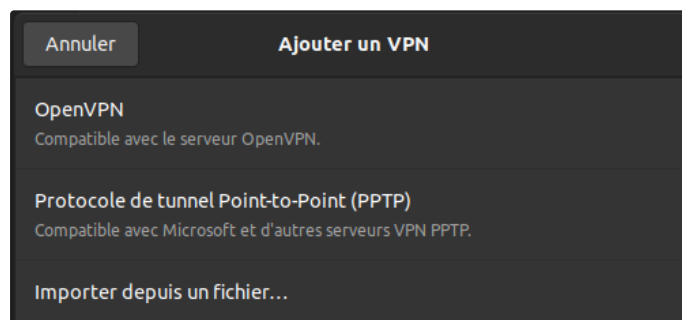
Finally, these steps must be followed in the order they are given, or the process will fail.

Install the novalix file VPN.

- Download the file here: [NovAliX.ovpn](#)
- Then got to Parameters > Network
- click on the '+' button on the VPN section:



- click on 'import' a file:



- select the file you downloaded, and you're ready to go.

NOTE: you will need a token from the infra department to make it work.

AnyDesk Windows to Ubuntu

To make it work, both need to install AnyDesk

Then the ubuntu user must edit this file :

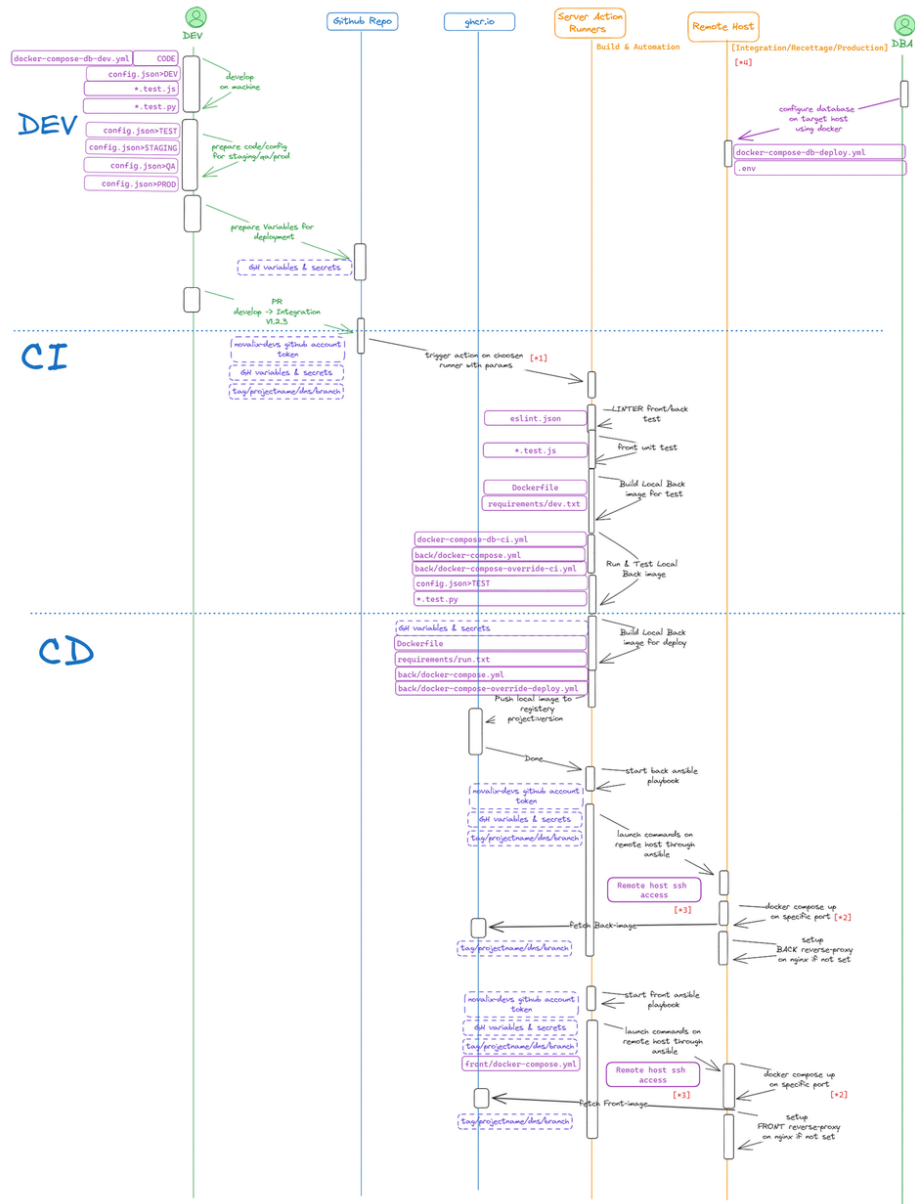
```
1 sudo vim /etc/gdm3/custom.conf
```

And uncomment the parameters `WaylandEnable` `AutomaticLoginEnable` and `AutomaticLogin`

```
1 # GDM configuration storage
2 #
3 # See /usr/share/gdm/gdm.schemas for a list of available options.
4
5 [daemon]
6 # Uncomment the line below to force the login screen to use Xorg
7 WaylandEnable=false
8
9 # Enabling automatic login
10 AutomaticLoginEnable = true
11 AutomaticLogin = user1
12
13 # Enabling timed login
14 # TimedLoginEnable = true
15 # TimedLogin = user1
16 # TimedLoginDelay = 10
17
18 [security]
19
20 [xdmcp]
21
22 [chooser]
23
24 [debug]
25 # Uncomment the line below to turn on debugging
26 # More verbose logs
27 # Additionally lets the X server dump core if it crashes
28 #Enable=true
```

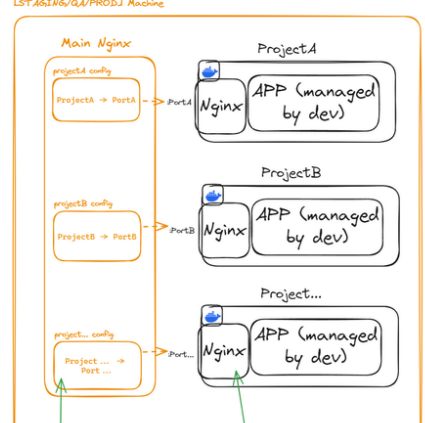
Then reboot computer

Some file = Code and configurations managed by DevOps Admin Need for sequence
 RECETTAGE CONFIG = Code and configurations managed by Developer needed for sequence

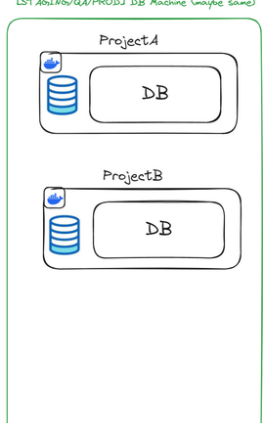


- [*1] irl will be fetched periodically by runner since the machine is internal
- [*2] port will be determined by the first available port on the machine
- [*3] Need the target remote host to have the ssh key of the ansible executor for seamless connexion
- [*4] Target Remote host account must have specific right for managing nginx, systemctl for nginx & docker

Managed by DevOps Admin + Infra
 [STAGING/QA/PROD] Machine



Managed by DBA
 [STAGING/QA/PROD] DB Machine (maybe same)





Link with development workflow is explained in our [Software Development Practices](#) Space here : [Which Dev Flow to use](#)

Installation logs for builder and server

Runner

1. Accounts

- Create sudo `runner` account

```
1 adduser runner
2 usermod -aG sudo username
```

2.0 Softwares


```
1 sudo apt-get update
2 sudo apt-get install git-all jq openssh-client
```

- **2.1** Setup github runner service: [Adding self-hosted runners - GitHub Enterprise Cloud Docs](#)
- **2.2** Configure the service : [Configuring the self-hosted runner application as a service - GitHub Docs](#)
- **2.3** Install docker & docker-compose ([Install Docker Engine on Ubuntu](#))

```
1 systemctl start docker
```

2.3.1 If docker daemon isn't started right away. Also add runner user to docker group. If you've got issues with `/var/run/docker.sock`, change its permissions to 666

- **2.4** Install `ansible-core` : [How To Install and Configure Ansible on Ubuntu 20.04 | DigitalOcean](#)

 Use the command `sudo apt install ansible-core` NOT ... `install ansible...`

- **2.5** Install ansible docker module

```
1 ansible-galaxy collection install community.docker
```

- **2.6** Create the networks for the workflows
- **2.7** Add labels needed to the runner on <https://github.com/organizations/novalixofficial/settings/actions/runners>
- **2.8** To start or restart the service :

```
1 sudo ./svc.sh start
```

Runner To Target SSH setup

- **3.1** Generate a ssh-key if not present already with `ssh-keygen`
- **3.2** For EACH target machine, you'll need to setup an ssh connection between them, like so

```
1 ssh-copy-id novalix@<target-dns>.novalix.com
```

Target Host :

Install on Linux ubuntu

1. Accounts

- 1.1 Account `novalix` with sudo permissions (add password in keepass if created)

```
1 adduser novalix
2 usermod -aG sudo username
```

2. Softwares

```
1 sudo apt-get update
2 sudo apt-get install git-all nginx openssh-client
```

- 2.1 docker & docker-compose ([🌐 Install Docker Engine on Ubuntu](#))

```
1 systemctl start docker
```

3. Nginx + SSL Certificates

3.1 Folder for Nginx and docker

```
1 sudo mkdir /etc/nginx/ssl
2 sudo mkdir /etc/nginx/nvlx_default.d
3 sudo mkdir /etc/nginx/nvlx_default.d/project
4 sudo mkdir /etc/nginx/nvlx_default.d/host
5 sudo touch /etc/nginx/nvlx_default.d/project/project_server.conf
6
7 docker volume create --driver local \
8   --opt type=none \
9   --opt device=/etc/nginx/nvlx_default.d/project \
10  --opt o=bind \
11  nvlx_default_project_nginx
```

3.2 Create default server file for all reverse proxies

3.2.1 Create `/etc/nginx/nvlx_default.d/host/project_nginx.conf`

```
1 # Continuous Delivery : is file will be injected
2 # IN every nginx main config IN every nginx container
3 # FOR each project
4
5 location /test{
6     add_header X-NOVALIXTEST config_is_injected_from_external_nginx_mount_inside_nginx_container_of_project;
7     add_header Content-Type "text/plain";
8     return 200 "check your header response";
9 }
```

3.2.2 Create `/etc/nginx/nvlx_default.d/host/project_server.conf`

```
1 # Continuous Delivery : this file will be injected
2 # IN every nginx server block IN every nginx container
3 # FOR each project
```

3.2.3 Create `/etc/nginx/nvlx_default.d/host/server.conf`

```
1 # Continuous Delivery : this file will be injected
2 # IN every reverse proxy server block
3 # FOR each project on the host
4
```

```
5 ssl_certificate /etc/nginx/ssl/novalix.cer;
6 ssl_certificate_key /etc/nginx/ssl/novalix.key;
```

3.2.4 Create /etc/nginx/nvlx_default.d/host/location.conf

```
1 # Continuous Delivery : this file will be injected
2 # IN every reverse proxy location tag
3 # FOR each project on the host
4
5 proxy_set_header Host $host;
6 proxy_set_header X-Real-IP $remote_addr;
7 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
8
9 # Websocket upgrade if needed
10 proxy_set_header Upgrade $http_upgrade;
11 proxy_set_header Connection "upgrade";
12 proxy_read_timeout 86400;
```

3.3 Folder permissions for ansible

- Run this script on the **target host** to allow the correct permission to our `novalix` account :

```
1 # create group
2 sudo groupadd ansible_execs
3
4 # assign user to necessary groups
5 sudo usermod -a -G ansible_execs,docker novalix
6
7 # own the correct folders
8 sudo chgrp -R ansible_execs /etc/nginx
9 sudo chmod g+w /etc/nginx -R
10 sudo chmod g+w /var/log/nginx/ -R
11 sudo chmod g+w /var/ -R
12
13 sudo mkdir /var/deployed.d
14 sudo chgrp -R ansible_execs /var/deployed.d
15 sudo chmod g+w /var/deployed.d -R
16
17 #setup docker dns for easier maintenance
18 echo "172.17.0.1    docker-local" | sudo tee -a /etc/hosts
19
20 # create our specific sudo command to use without password
21 echo "%ansible_execs ALL=NOPASSWD: /bin/systemctl reload nginx" | sudo tee /etc/sudoers.d/ansible_execs
22 echo "%ansible_execs ALL=NOPASSWD: /bin/nginx -t" | sudo tee -a /etc/sudoers.d/ansible_execs
```

3.4 Nginx + SSL Certificates

- When asking for a new certificate, the **Infra Team** generate a **key** and will give it to the authority that will generate the **new certificate (and paste them here : [SSL Certificates](#))**

The extensions of those two files may vary (*.key / *.cer / *.cert / *.csr / *.pem) and doesn't matter s long as it contains a text file looking like a private key.

You will need to paste those file :

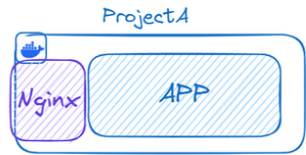
- The generated key (ideally *.key) → /etc/nginx/ssl/novalix.key
- The provided certificate (ideally *.cer) → /etc/nginx/ssl/novalix.cer

- All of the project managed by the CI/CD will be using the `*.novalex.com` certificate as SSL, for other SSL needs, contact the DevOps referent and Infra Team.

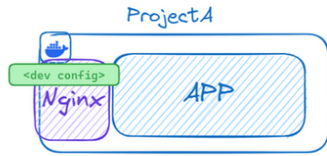
4. 🐱‍💻 Target to GitHub SSH Setup

- `ssh-keyscan github.com >> /home/runner/.ssh/known_hosts`
- Generate a ssh-key if not present already with `ssh-keygen`
- Make sure that the generated **public key** is registered on the [novalex-devs github account](#)

By default, there is an nginx configuration for your app

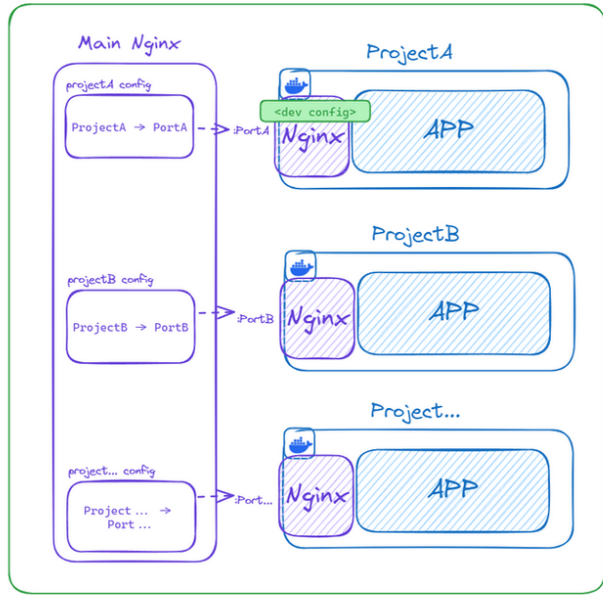


But developer can require special configuration(file upload, timeout, etc...)



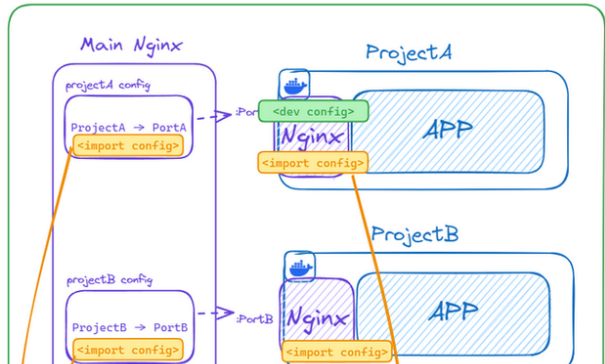
However, the nginx config is not isolated and is dependent on the target machine nginx config

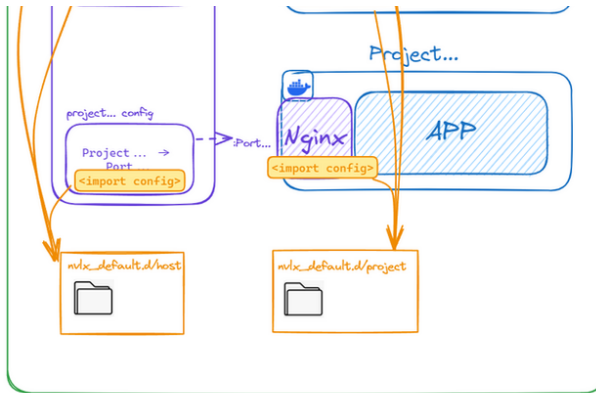
[STAGING/QA/PROD] Machine



To allow a DevOps Admin to manage all client config, we configured specific entry point for the nginx configuration

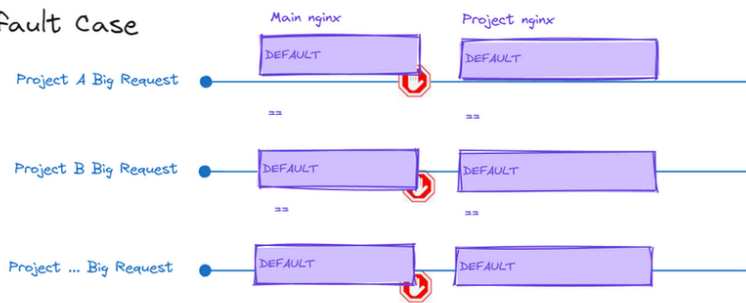
[STAGING/QA/PROD] Machine



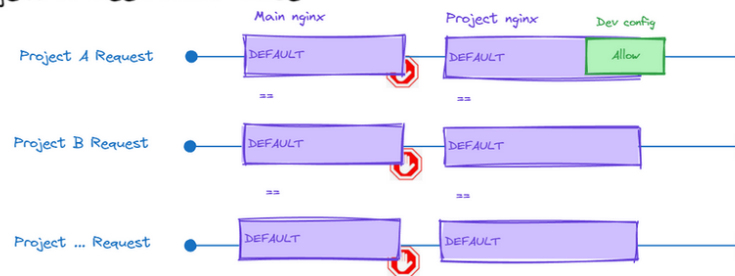


If we schematize the configurations by "allow" and "restrict", we can see that there is several checkpoints to manage to avoid security flaws

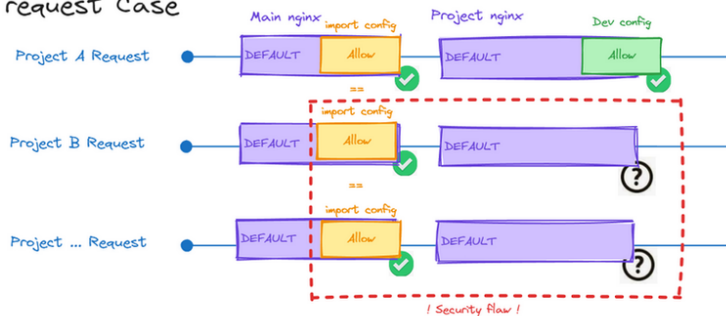
Default Case



Project A Need Allow Case



Permit Big request Case



Permit Big request only for Project A Case

