ADLIN

Devoir Maison

SRS Promo 2026

Clément Lanata

06 mars 2025

Contents

1 Sujet

Vous devez mettre en place un ou plusieurs *playbooks* Ansible permettant le déploiement automatisé d'un système d'information comprenant :

- la gestion de noms de domaine ;
- la gestion de plusieurs sites web ;
- une supervision.

Un numéro vous a été remis lors d'un précédent cours. Il correspond à votre ordre dans l'ordre alphabétique de votre promo. Retenez bien ce numéro, vous en aurez besoin pour la construction de votre infrastructure.

1.1 Préambule et prérequis

1.1.1 Prérequis matériel

Pour l'ensemble de votre infrastructure, 4 Go de RAM sont nécessaire ainsi que maximum 100 Go d'espace de stockage. Pensez à provisionner justement vos VM. Le tableau suivant devrait correctement vous guider.

Type de VM	vCPU	RAM (Mo)	Stockage (Go)
SNS	1	1024	10
VM client	2	2048	24
VM serveur	1	512	16

SNS signifie Stormshield Network Security, la solution de pare-feu de l'entreprise française Stormshield.

La machine virtuelle et sa license sont disponibles ici.
Veuillez à choisir le fichier qui correspond à votre hyperviseur. Pour rappel, l'ova est pour Vmware ESXi ou Virtual Box.

1.1.2 Hyperviseur

Enfin, il est conseillé de faire votre infrastructure sous *Vmware Workstation 16* ou *17*. Cependant, si vous souhaitez la faire avec un autre système de virtualisation (*Proxmox, Vmware ESXi, Oracle VM VirtualBox, libvirt, etc*), vous êtes libre de choisir votre hyperviseur.

1.1.3 Machine Vitruelle

Vous utiliserez des machines virtuelles sous Debian 12. Vous pouvez les déployer de manière automatisée mais il ne s'agit pas d'une nécessité.

1.1.4 Compte à utiliser

Vous utiliserez un compte nommé `ansible` pour déployer vos roles. Ce compte n'a pas besoin d'être créer par Ansible. Pour le rendu, considérer qu'il existe déjà et que vous pouvez vous y connecter. Pour votre infrastructure, pensez à le créer et à le mettre dans le groupe `sudo`.

1.1.5 Rôles

Il est interdit d'utiliser des rôles externes. Ainsi donc, vous devrez créer tous les rôles que vous allez utiliser. Pensez à faire des rôles le plus générique possible. L'attention que vous porterez à rendre vos rôles les plus variabilisés possible sera très appréciée.
Il est cependant possible d'utiliser des collections externes (exemple: `community.docker`). Pensez à faire un fichier `requirements.yml` dans ce cas.

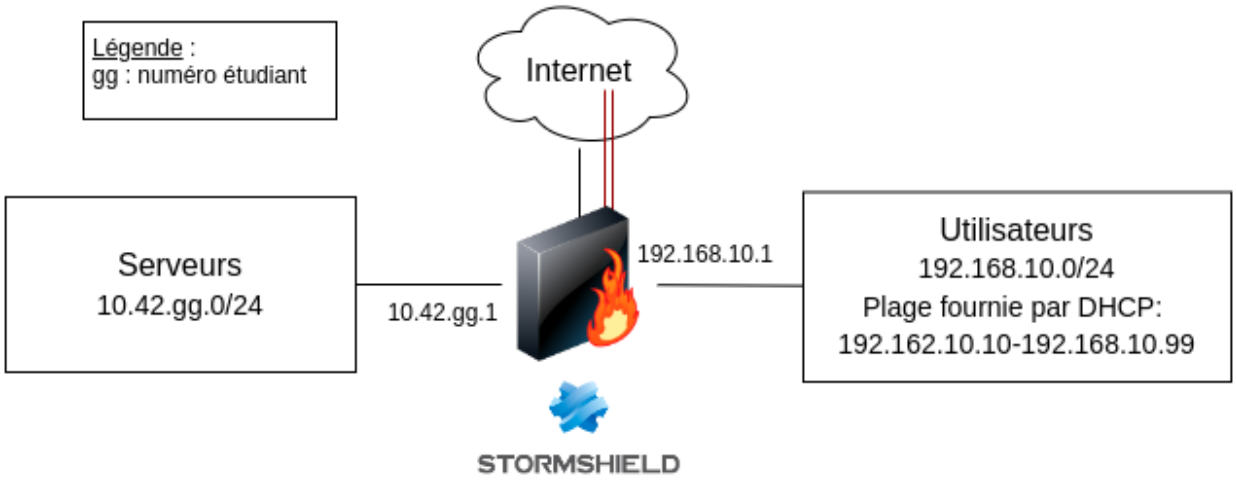
1.1.6 Idempotance

De plus, l'idempotance de vos rôles est très importante. Vous souhaitez savoir si l'état de vos services a été modifié suite à l'exécution de votre *playbook*.

1.2 Infrastructure réseau

> Aucun rôle *Ansible* n'est demandé pour cette section.

Voici un schéma de l'infrastructure que vous allre mettre en place sur votre hyperviseur:



Le pare-feu Stormshield distribue deux réseaux :

- Un LAN serveur (`10.42.gg.0/24`) qui hébergera autant de machines virtuelles que vous souhaitez. Leur adresses IP seront statiques. L'interface portera l'adresse `10.42.gg.1/24` et sera nommée `dmz_lan` ;
- Un LAN utilisateur (`192.168.10.0/24`) qui hébergera un unique client. Son adresse et sa configuration réseau sont fournies par DHCP. L'interface portera l'adresse `192.168.10.1/24` et sera nommée `user_lan`.

Le pare-feu hébergera un serveur DHCP, fournissant des adresses dans la plage 192.168.10.10 - 192.168.10.100 sur son interface du réseau utilisateur. La configuration du DNS doit également être fourni par DHCP.

L'ensemble de vos machines virtuelles ne doit pas être mis en pause, en particulier le pare-feu. Préférer systématiquement l'extinction des VM à leur mise en pause.

1.3 Tunnel IPsec

Aucun rôle *Ansible* n'est demandé pour cette section.

Un tunnel IPsec sera monté entre votre pare-feu et le concentrateur IPsec d'ADLIN disponible sur Internet (`141.94.222.99`). Il permet la communication entre votre LAN serveur et l'infrastructure d'ADLIN, qui héberge un DNS et permet les corrections.
La configuration du *Peer* doit correspondre aux spécifications suivantes :

Paramètre	Valeurs
Nom	`Site_VPS`
Remote Gateway	141.94.222.99
Local Address	*Any*
IKE profile	*StrongEncryption*
IKE version	IKEv2
Authentication method	*Preshared Key (PSK)*
PSK	`ADLINIsBetterThanACDA!`
DPD	*Low*
DSCP	*Best effort*

La configuration du tunnel doit correspondre aux spécifications suivantes :

Paramètre	Valeurs
Local network	`Network_dmz_lan`
Peer	`Site_VPS`
Remote netwotk	`100.64.51.1`
Encryption profile	*StrongEncryption*
Keep alive	30

Enfin, l'IP `100.64.51.1` doit être capable de contacter l'IP `10.42.gg.1` en ICMP echo.

1.4 DNS

Maintenant que le socle réseau est prêt, nous allons commencer à déployer des services avec Ansible. Le service le plus indispensable dans un système d'information est le DNS, nous commencerons par là. L'ensemble des vos infrastructures sont des sous-domaines du domaine `srs.adlin`. Ainsi, vous allez chacun avoir un sous-domaine pour exposer vos différents services.

Il faut que votre DNS soit atteignable avec l'IP `10.42.gg.2`.

Votre DNS sera autoritaire sur le nom de domaine `<numéro>.srs.adlin`. Par exemple, si je suis le numéro 9, mon sous-domaine est `9.srs.adlin`. De plus, votre DNS doit être récursif sur l'ensemble des autres domaines. Ainsi, il devient le serveur DNS de votre infrastructure et est en capacité de résoudre les sous-domaines de `srs.adlin` comme `google.com` ou `cyber.gouv.fr`.

Afin que votre domaine soit atteignable par les autres étudiants, il est nécessaire que vous l'exposiez au serveur DNS maître sur le domaine `srs.adlin` en `100.64.51.1`. Que faut-il faire sur votre pare-feu pour que votre serveur DNS soit atteignable depuis l'extérieur ? De

plus, le serveur DNS `srs.adlin` possède une zone qui est secondaire à votre domaine et ainsi, même lorsque votre infrastrucutre est éteinte, est capable de résoudre vos noms de domaine. Pensez donc à laisser la possibilité à ce serveur de faire un transfert de zone. Enfin, penser à ajuster correctement les metadonnées de votre *Start of Autority*, vous souhaitez que le serveur secondaire aille régulièrement récupérer vos noms de domaine mais que ces noms n'expirent pas trop vite.

Vous êtes libre sur le choix de la technologie de DNS, tant qu'il ne s'agit pas d'un service DNS sous *Windows Server*.

Vous devez créer un/des rôle(s) Ansible pour déployer et configurer votre serveur DNS de manière dynamique (avec des variables pour pouvoir réutiliser votre rôle) et idempotante.

1.5 Webserver

Maintenant que votre service DNS est prêt, nous allons nous en servir. Vous allez déployer plusieurs services web qui seront exposés au public (ici, l'ensemble de la classe). Ces services répondront aux noms de domaines suivants :

- `web1.xx.srs.adlin` ;
- `web2.xx.srs.adlin` ;
- `web3.xx.srs.adlin` ;
- `web4.xx.srs.adlin` ;
- `ilovecats.xx.srs.adlin`.

Par exemple, si je suis le numéro 9, mes domaines seront `web1.9.srs.adlin`, etc. Ces cinqs sites devront être accessible en HTTPS pour le reste de la classe avec les domaines précédents. Les quatre sites sous le nom `web` devront afficher une page de texte, distincte pour chacun des sites. Le site `ilovecats` devra afficher une image de chat.

Afin que le site soit accessible en HTTPS, il y a deux prérequis. Tout d'abord, vous devez mettre le certificat racine de l'autorité de certification dans vos bases de confiance (disponible ici). Ensuite, vous trouverez un serveur ACME (*Automated Certificate Management Environment*) à l'adresse `https://acme.srs.adlin:9000`. S'agissant d'un service similaire à *Let's Encrypt*, vous pouvez par exemple utiliser `certbot`.

Si vous souhaitez utiliser `certbot`, penser à utiliser l'option `--server https://acme.srs.adlin:9000/acme/acme/directory` sinon le binaire ira voir les serveurs de *Let's Encrypt*.

Le choix de la technologie de site web est libre, tant qu'il ne s'agit pas d'un service IIS sous *Windows Server*. Ce choix devra être justifié dans le README.

1.6 Supervision

Vous avez enfin un système d'informations avec un nom de domaine opérationnel et des services utilisateurs.

Nous allons maintenant superviser tout cela, afin d'être au courant le plus tôt possible d'une panne sur le SI et de pouvoir réagir avant que les utilisateurs viennent se plaindre.

Tout d'abord, faites la liste de tous les composants essentiels aux services qui vous rendez. Il s'agit des composants réseaux, matériels et logiciels vitaux de votre SI. Une fois cette liste établie, vous allez devoir mettre en place des services de supervision pour connaitre en temps réel l'état de votre système d'information.

Ces états devront être visualisable facilement et rapidement via des tableaux de bord. Vous devrez mettre en place un minimum un tableau de bord par type de composant :

- réseau ;
- DNS ;
- web.

Enfin, vous devrez faire un tableau de bord général et succinct permettant de connaitre l'état de votre SI en un coup d'oeil.

Votre plateforme de supervision devra être accessible (pour le test de fonctionnalité) à travers le VPN en HTTPS sous le nom de domain `supervision.xx.srs.adlin`. Le certificat devra bien évidemment être valide. Un compte avec des droits en lecture seule nommée `audit` devra être présent, avec le mot de passe :

`ShouldWeCreateATimeMachineAndKillBillG@tes?`

2 Rendu et notation

Votre DM sera à rendre au plus tard le **vendredi 22 juin 23h42** à l'adresse :

- clement.lanata@epita.fr

L'objet de votre mail devra être : `[ADLIN][DM] login`.

Aucun retard ne sera toléré.

Votre rendu devra déployer toute votre infrastructure (DNS, web server, supervision). Le déploiement peut se faire dans l'ordre que vous préférez. Vous pouvez par exemple faire l'une ou l'autre des procédures ci-dessous :

- déployer votre DNS avec tous les noms de domaines puis déployer les serveurs web ;
- déployer votre DNS avec simplement votre sous-domaine, déployer les serveurs web puis ajouter les noms de domaines en `web`.

L'important est qu'à la fin du déploiement, le résultat soit là.

Vous pouvez considérer que les machines virtuelles sont déjà présentes sous Debian 12 avec un accès au miroir Debian par défaut. Le compte `ansible` est présent sur les VM avec des droits `sudo`.

Vos rôles et *playbook* doient être variabilisés au maximum et idempotents.

2.1 Architecture de rendu

Le rendu se fera sous la forme d'une **tarball compressée** (pas un zip, pas un rar) sous le nom `ADLIN-DM-login.tar.gz` ayant l'architecture ci-après :

```
|-- ansible.cfg      (optionnel)
|-- inventory
|   '-- *.yml
|-- playbook.yml
|-- README.txt       (ou markdown)
|-- requirements.yml (optionnel)
'-- roles
    |-- role1
    |   '-- ...
    '-- role2
        '-- ...
```

Le contenu de votre `README` peut être en français ou en anglais.

2.2 Test de votre infrastructure

Un test de votre infrastructure aura lieu dans la foulée du dernier cours. Une date et un créneau vous seront communiqués.

Durant ce laps de temps, vos infrastructures devront être allumées afin de vérifier que tous les services demandés soient implémentés et opérationnels.

2.3 Construction de la note

Voici comment se construira votre note pour ce cours :

- 80% pour les DMs (environ 20% par DM) ;
- 20% pour le test de fonctionnement ;
- +5% pour un retour sur le cours (dans le `README`).