

TP Administration Système et Devops 1

Configuration de base, DNS et premiers sites web

Responsable

Philippe SWARTVAGHER
philippe.swartvagher@enseirb-matmeca.fr

Intervenants

Tom CLAUDEL
tom.claudel@u-bordeaux.fr

2025 – 2026

Vous avez chacun et chacune une machine virtuelle (VM) qui vous est dédiée, que vous allez configurer et dans laquelle vous allez installer différents services. Vous allez utiliser cette même VM au cours des différents TPs. Sur certains aspects, les TPs sont dépendants les uns des autres.

Vous allez aller gérer votre VM via SSH, depuis les machines (physiques) des salles réseau. Pour cela, vous utiliserez la partition TP **Reserves**. Identifiez avec l'utilisateur **user** qui a pour mot de passe **retel**.

Attention : Cette session sera également utilisée par un de vos camarades de l'autre demi-groupe.

Les informations que vous avez besoin de connaître concernant votre VM :

- L'IP est disponible dans le mail que vous avez reçu et sans doute que le chargé TP projette l'information.
- Votre compte utilisateur :
 - Nom d'utilisateur : votre login CAS
 - Mot de passe : votre login CAS
- Mot de passe de l'utilisateur **root** : **root**
- Ne modifiez pas ces mots de passe ! Cela facilitera d'éventuels débogages.

Rappel : Vous êtes dans les salles réseau où tout le monde peut faire n'importe quoi avec le réseau et tout le monde peut être **root** sur les machines. Ce n'est donc absolument pas un environnement de confiance. Ne saisissez donc pas des informations sensibles (votre mot de passe CAS, par exemple).

1 Connexion et configuration SSH

1. Pinguez l'IP de votre VM et assurez-vous d'obtenir une réponse.

2. Connectez-vous une première fois en SSH à votre VM, en utilisant votre compte utilisateur (pas `root`).
3. **Sur votre machine physique**, générez une clé SSH.
 - Précisez l'option `-f /home/user/.ssh/login_ed25519` pour préciser le nom de la clé (un de vos camarades va également générer sa clé SSH sur cette session).
 - Il n'est pas nécessaire de mettre de passphrase pour ces TPs (appuyez simplement sur `Entrée` lorsque la question vous est posée).
4. Déposez la clé publique dans votre VM.
5. Connectez-vous à nouveau en SSH à votre VM, cette fois-ci en utilisation l'authentification par clé.
 - Votre clé SSH n'a pas un nom standard, et vous ne l'avez pas encore utilisée : il faudra préciser à `ssh` quelle clé utiliser.
 - SSH ne doit plus vous demander le mot de passe de votre compte sur votre VM.
6. Pour faciliter la connexion SSH, configurez SSH de façon à ce que `ssh $login` se connecte à votre VM en utilisant l'authentification par clé.

2 Qu'avons-nous dans ces VMs ?

1. De quelle distribution Linux s'agit-il ?
 - Le fichier `/etc/os-release` contient la réponse.
2. Quelle version de Linux est utilisée ?
 - La commande `uname -a` vous donnera la réponse.
3. Quelle quantité de mémoire RAM a la VM ?
4. Combien de cœurs a la VM ?
 - `nproc` ou le fichier `/proc/cpuinfo` vous donneront la réponse.
5. Comment est organisé le stockage ? De quelle quantité de stockage disposez-vous ?
 - `df -h` ou `lsblk` vous donneront la réponse.
6. Êtes-vous un utilisateur qui a le droit d'employer la commande `sudo` ?
 - La commande pour afficher les groupes auxquels on appartient est `groups`.
7. Quelle est la configuration IP de la VM (adresse, passerelle, serveurs DNS) ?
 - Ajoutez la ligne `nameserver 172.18.[13].33` au fichier qui va bien.
 - Assurez-vous que vous pouvez pinguer `www.bordeaux-inp.fr`.
8. Y a-t-il d'autres utilisateurs ?
 - Les utilisateurs locaux sont listés dans le fichier `/etc/passwd`. À quoi correspondent toutes les informations dans ce fichier ?
 - Quelle autre possibilité (moins complète) avons-nous pour lister les utilisateurs ?

3 Manipulation de paquets

1. Pour ce TP, vous avez à disposition un serveur de cache pour les paquets. Modifiez l'IP définie dans `/etc/apt/apt.conf` en `172.18.[13].31` pour pointer vers le serveur de cache.
 - L'éditeur de texte `nano` est déjà installé.
 - Il faut avoir les droits `root` pour éditer ce fichier.
2. Si nécessaire, mettez à jour les paquets installés sur votre VM.
3. Installez le paquet `htop`.
4. Exécutez `htop`.
 - Les informations affichées sont-elles cohérentes avec celles obtenues précédemment ?
 - `Q` pour quitter.

4 Sécuriser le serveur SSH

Tout se joue dans le fichier `/etc/ssh/sshd_config`.

1. Changez le numéro de port sur lequel écoute le serveur SSH.
 - Décommentez la ligne `#Port 22`
 - Choisissez n'importe quel nombre supérieur à 1024.
 - Il ne faudra pas oublier de mettre à jour votre raccourci SSH pour vous connecter.
2. Interdisez la connexion avec l'utilisateur `root`.
 - `PermitRootLogin` doit prendre la valeur `no`.
3. Interdisez l'authentification par mot de passe.
 - `PasswordAuthentication` doit prendre la valeur `no`.
4. Sauvegardez les modifications apportées au fichier, puis quittez.
5. Assurez-vous que la syntaxe du fichier de configuration est correcte avec la commande `sshd -t` exécutée en tant que `root`.
6. Rechargez le service `ssh` pour que les changements de configuration soit pris en compte.
7. Vous devez réussir à vous connecter en SSH à votre VM depuis un autre terminal.
 - Depuis un autre terminal, tout en conservant la session SSH que vous avez dans le premier terminal, pour pouvoir corriger le problème si vous ne parvenez pas à vous connecter.

5 Un premier service lancé manuellement

1. Dans votre `$HOME` sur votre VM, créez un simple fichier HTML, avec un contenu minimal.

2. Depuis votre `$HOME`, lancez le serveur HTTP fourni avec Python :
`python3 -m http.server`
3. Ouvrez votre navigateur web et chargez la page HTML que vous venez de créer.
 - Quelle adresse faut-il saisir dans la barre d'adresse du navigateur ?
4. Arrêtez le serveur HTTP avec `Ctrl`+`C`.

6 Votre zone DNS

Vous allez mettre en place un serveur DNS qui fait autorité sur votre zone. Pendant ces TP, le serveur DNS `172.18.[13].33` est résolveur, mais fait aussi autorité sur la zone `g[12].t2.` et délègue les zones `login.g[12].t2.` vers votre VM.

1. Si ce n'est pas déjà fait, changez le résolveur DNS de votre machine (physique) pour utiliser le serveur DNS mentionné ci-dessus.
2. Assurez-vous que vous pouvez toujours résoudre `www.bordeaux-inp.fr`.
 - Si `dig` n'est pas installé, il est dans le paquet `bind9-dnsutils`.
3. Sur votre VM, installez le paquet `bind9`.
4. Dans le fichier `/etc/bind/named.conf.local`, définissez la zone sur laquelle votre serveur aura autorité :

```
zone "login.g[12].t2" {
    type primary;
    file "/etc/bind/login.g[12].t2";
    notify false;
};
```

5. Définissez ensuite les entrées de la zone dans le fichier correspondant :

```
$TTL 2d      ; default TTL for zone
$ORIGIN login.g[12].t2. ; base domain-name
@   IN  SOA  login.g[12].t2. hostmaster.login.g[12].t2.
    (
      2026031201 ; serial number
      12h        ; refresh
      15m        ; update retry
      4d         ; expiry
      2h         ; minimum
    )

    IN  NS   ns
    IN  A    <IP de votre VM>
ns    IN  A    <IP de votre VM>
```

6. Vérifiez la configuration avec `named-checkconf` et `named-checkzone login.g[12].t2 /etc/bind/login.g[12].t2`.
7. Redémarrez le service `bind9`.
8. Résolvez `login.g[12].t2` et `ns.login.g[12].t2` depuis votre machine, assurez-vous que l'IP de votre VM est bien renvoyée.

7 Un premier site web

Nous allons installer un serveur web, pour que le nom de domaine `login.g[12].t2` corresponde à un simple site web (par exemple la page HTML que vous avez écrite pour le test avec Python).

1. Installez le paquet `nginx`.
2. Créez le fichier `/etc/nginx/sites-available/login` avec le contenu suivant (il s'agit d'un copier/coller de la fin du fichier `/etc/nginx/sites-enabled/default`), qui va configurer le *virtual host* pour votre nom de domaine :

```
server {
    listen 80;
    listen [::]:80;

    server_name login.g[12].t2;

    root /var/www/login/;
    index index.html;

    location / {
        try_files $uri $uri/ =404;
    }
}
```

- À quoi correspondent les différentes instructions dans ce fichier ?
3. Créez un lien symbolique `/etc/nginx/sites-enabled/login` vers `/etc/nginx/sites-available/login`.
 4. Vérifiez que la configuration Nginx est correcte avec `nginx -t`.
 5. Rechargez le service `nginx`.
 6. Créez le dossier `/var/www/login` et placez-y votre fichier HTML, idéalement nommé `index.html`.
 - Les fichiers servis par Nginx doivent être lisibles par l'utilisateur `www-data`.
 7. Depuis votre navigateur, accédez à votre site web.
 8. En parcourant les fichiers de configuration dans `/etc/nginx`, trouvez où sont enregistrés les logs de Nginx.
 - La commande `grep` avec les options `-lIn` (que font ces options ?) vous sera sans doute utile.
 9. Consultez les fichiers de logs de Nginx. Que voyez-vous ?

8 Un peu de surveillance

Pour surveiller l'activité de notre VM, nous allons utiliser l'outil Munin. Il repose sur une architecture client/serveur : toutes les 5 minutes, le serveur se connecte à l'ensemble de clients configurés pour récupérer les informations des sondes configurées par les clients.

Les sondes rapportent des valeurs numériques sur l'état actuel du système : nombre de processus, mémoire utilisée, espace disque utilisé, ... Pour ce TP, serveur et client seront installés sur la même VM.

Par défaut, le serveur Munin considère qu'un client est également installé localement (regardez dans `/etc/munin/munin.conf`), ce qui correspond à notre cas, et génère des pages HTML avec des graphiques dans le dossier `/var/cache/munin/www/`. L'objectif est d'avoir l'interface web de supervision depuis l'adresse `munin.login.g[12].t2`.

1. Installez les paquets `munin`, `munin-node` et `munin-plugins-extra`.
2. La commande `sudo munin-node-configure --suggest` vous montre quelles sont les sondes (plugins) disponibles, celles qui sont déjà activées, et pourquoi certaines sont désactivées. L'ensemble des plugins déjà activés sera suffisant pour commencer.
3. Ajoutez l'entrée `munin` dans votre zone DNS et rechargez le service `bind`. Assurez-vous que `munin.login.g[12].t2` est correctement résolu.
4. Comme vous l'avez fait pour `login.g[12].t2`, créez un virtual host Nginx pour `munin.login.g[12].t2` qui servira les fichiers du dossier `/var/cache/munin/www/`.
5. Dans votre navigateur, rendez-vous à l'adresse `http://munin.login.g[12].t2` pour contempler les graphiques.

9 Pour les plus rapides

9.1 Mise en place d'un pare-feu

1. Exécutez la commande `sudo netstat -laptuten` fournie par le paquet `net-tools`. Que vous montre-t-elle ?
2. Installez et configurez le pare-feu `ufw`.
 - Consultez de la documentation en ligne.
 - Généralement on autorise tout le trafic sortant et on restreint le trafic entrant sur les ports légitimes.
 - Attention à ne pas vous enfermer dehors !

9.2 Encore plus de monitoring

1. À partir des informations fournies par la commande `sudo munin-node-configure --suggest`, activez plus de sondes.
 - On active un plugin en faisant un lien symbolique de `/etc/munin/plugins/<plugin>` vers `/usr/share/munin/plugins/<plugin>`.
2. En suivant l'exemple de configuration de la documentation de Munin ¹, rendez fonctionnel le zoom dans les graphiques sur les pages web.

1. <https://guide.munin-monitoring.org/en/latest/example/webserver/nginx-cron.html>

9.3 Redondance de votre zone DNS

1. Votre serveur DNS est le serveur primaire qui a autorité sur votre zone DNS. Configurez votre serveur DNS pour qu'il soit le serveur DNS secondaire ayant autant d'autorité sur la zone DNS de votre camarade. Réciproquement, votre camarade devra configurer son serveur DNS pour autoriser le transfert de sa zone vers votre serveur.
2. Vérifiez avec `dig` que votre serveur sait résoudre les noms de domaines de la zone de votre camarade et réciproquement.