

TUTORIEL ANSIBLE

Configurer Apache2 RemoteIP derrière un reverse proxy Nginx

Intégration dans le rôle LAMP-COMPLET

Objectif : Apache doit journaliser l'adresse IP réelle du visiteur et non l'adresse IP du reverse proxy Nginx. Nginx est déjà configuré pour transmettre X-Forwarded-For.

1. Contexte

Reverse proxies de confiance : 172.16.0.110 et 192.168.10.121

- Le rôle Ansible utilisé est : /etc/ansible/roles/LAMP-COMPLET/
- Le fichier principal modifié est : tasks/main.yml
- Le module Apache utilisé est : mod_remoteip
- Le header utilisé pour récupérer l'IP d'origine est : X-Forwarded-For

```
- name: Activer le module Expires Apache
  community.general.apache2_module:
    name: expires
    state: present
  notify: Redemarrer Apache

- name: Activer le module Deflate Apache
  community.general.apache2_module:
    name: deflate
    state: present
  notify: Redemarrer Apache

- name: Activer le module Apache remoteip
  community.general.apache2_module:
    name: remoteip
    state: present

- name: Créer la configuration Apache remoteip
  ansible.builtin.copy:
    dest: /etc/apache2/conf-available/remoteip.conf
    content: |
      RemoteIPHeader X-Forwarded-For
      RemoteIPTrustedProxy 172.16.0.110
      RemoteIPTrustedProxy 192.168.10.121
    owner: root
    group: root
    mode: "0644"

- name: Activer la configuration remoteip
  ansible.builtin.command:
    cmd: a2enconf remoteip
  register: remoteip_conf
  changed_when: "'Enabling conf remoteip' in remoteip_conf.stdout"
# =====
# VIRTUALHOST SSL PAR DEFAUT
```

Première intégration de RemoteIP dans tasks/main.yml.

2. Ajouter RemoteIP dans le rôle LAMP-COMPLET

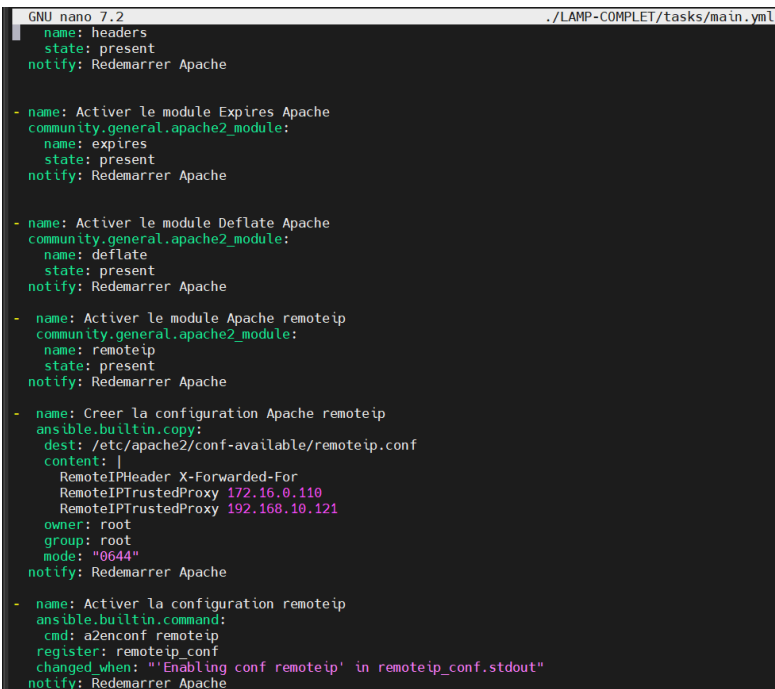
Dans `/etc/ansible/roles/LAMP-COMPLET/tasks/main.yml`, ajouter les trois tâches suivantes après les modules Apache déjà activés.

```
- name: Activer le module Apache remoteip
  community.general.apache2_module:
    name: remoteip
    state: present
  notify: Redemarrer Apache

- name: Creer la configuration Apache remoteip
  ansible.builtin.copy:
    dest: /etc/apache2/conf-available/remoteip.conf
    content: |
      RemoteIPHeader X-Forwarded-For
      RemoteIPTrustedProxy 172.16.0.110
      RemoteIPTrustedProxy 192.168.10.121
    owner: root
    group: root
    mode: "0644"
  notify: Redemarrer Apache

- name: Activer la configuration remoteip
  ansible.builtin.command:
    cmd: a2enconf remoteip
  register: remoteip_conf
  changed_when: "'Enabling conf remoteip' in remoteip_conf.stdout"
  notify: Redemarrer Apache
```

Pourquoi mettre notify sur les trois tâches ? Si le module, le fichier ou l'activation change, Apache doit relire sa configuration. Même si plusieurs tâches notifient le handler, Ansible ne redémarre Apache qu'une seule fois à la fin.



```
GNU nano 7.2                                ./LAMP-COMPLET/tasks/main.yml
name: headers
state: present
notify: Redemarrer Apache

- name: Activer le module Expires Apache
  community.general.apache2_module:
    name: expires
    state: present
  notify: Redemarrer Apache

- name: Activer le module Deflate Apache
  community.general.apache2_module:
    name: deflate
    state: present
  notify: Redemarrer Apache

- name: Activer le module Apache remoteip
  community.general.apache2_module:
    name: remoteip
    state: present
  notify: Redemarrer Apache

- name: Creer la configuration Apache remoteip
  ansible.builtin.copy:
    dest: /etc/apache2/conf-available/remoteip.conf
    content: |
      RemoteIPHeader X-Forwarded-For
      RemoteIPTrustedProxy 172.16.0.110
      RemoteIPTrustedProxy 192.168.10.121
    owner: root
    group: root
    mode: "0644"
  notify: Redemarrer Apache

- name: Activer la configuration remoteip
  ansible.builtin.command:
    cmd: a2enconf remoteip
  register: remoteip_conf
  changed_when: "'Enabling conf remoteip' in remoteip_conf.stdout"
  notify: Redemarrer Apache
```

Bloc RemoteIP final correctement indenté dans le rôle.

3. Comprendre ce que fait chaque tâche

3.1 Activer le module remoteip

```
community.general.apache2_module:
  name: remoteip
  state: present
```

Ansible vérifie que le module Apache **remoteip** est activé. S'il l'est déjà, la tâche reste en état ok.

3.2 Créer remoteip.conf

```
RemoteIPHeader X-Forwarded-For
RemoteIPTrustedProxy 172.16.0.110
RemoteIPTrustedProxy 192.168.10.121
```

Apache fait confiance au header X-Forwarded-For uniquement lorsque la requête provient de l'un des deux Nginx déclarés comme proxies de confiance.

3.3 Activer la configuration Apache

```
cmd: a2enconf remoteip
register: remoteip_conf
changed_when: "'Enabling conf remoteip' in remoteip_conf.stdout"
```

La commande active le fichier dans **/etc/apache2/conf-enabled/**. Le `changed_when` évite de considérer la tâche comme modifiée lorsque la configuration est déjà active.

```
content: |
  RemoteIPHeader X-Forwarded-For
  RemoteIPTrustedProxy 172.16.0.110
  RemoteIPTrustedProxy 192.168.10.121
owner: root
group: root
mode: "0644"

- name: Activer la configuration remoteip
  ansible.builtin.command:
    cmd: a2enconf remoteip
  register: remoteip_conf
  changed_when: "'Enabling conf remoteip' in remoteip_conf.stdout"
  notify: Redemarrer Apache
```

Étape intermédiaire : le notify doit être au même niveau YAML que register et changed_when.

```

GNU nano 2.2 /LAMP-COMPLET/tasks/main.yml
notify: Redemarrer Apache

- name: Activer le module Apache remoteip
  community.general.apache2_module:
    name: remoteip
    state: present

- name: Créer la configuration Apache remoteip
  ansible.builtin.copy:
    dest: /etc/apache2/conf-available/remoteip.conf
    content: |
      RemoteIPHeader X-Forwarded-For
      RemoteIPTrustedProxy 172.16.0.110
      RemoteIPTrustedProxy 192.168.10.121
    owner: root
    group: root
    mode: "0644"
  notify: Redemarrer Apache

- name: Activer la configuration remoteip
  ansible.builtin.command:
    cmd: a2enconf remoteip
    register: remoteip_conf
    changed_when: "'Enabling conf remoteip' in remoteip_conf.stdout"
  # =====
  # VIRTUALHOST SSL PAR DEFAULT
  # Equivalent : a2ensite default-ssl
  # =====

- name: Activer le site SSL par défaut
  ansible.builtin.command:
    cmd: a2ensite default-ssl
    creates: /etc/apache2/sites-enabled/default-ssl.conf
  notify: Redemarrer Apache

# =====
# SERVICES
# =====

```

Correction de l'indentation et ajout du notify sur les changements RemoteIP.

4. Erreur rencontrée : indentation YAML

Une erreur de syntaxe a été rencontrée : **did not find expected '-' indicator**

La cause était l'alignement de **notify**. En YAML, les clés appartenant à une même tâche doivent être au même niveau.

```

- name: Exemple correct
  community.general.apache2_module:
    name: remoteip
    state: present
  notify: Redemarrer Apache

```

Règle simple : - name, le module, register, changed_when et notify sont au niveau de la tâche. Les paramètres name/state du module sont indentés un niveau plus loin.

Avant d'exécuter réellement le rôle, on peut contrôler la syntaxe :

```
ansible-playbook /etc/ansible/playbooks/lamp.yml --syntax-check
```

5. Exécuter le playbook

Lancer le playbook LAMP :

```
ansible-playbook /etc/ansible/playbooks/lamp.yml
```

Lors du premier passage, les tâches RemoteIP sont en **changed** car le module, le fichier et la configuration sont ajoutés. Le handler redémarre ensuite Apache une seule fois.

```
root@ANSIBLE-SRV-01:/etc/ansible/roles# ansible-playbook /etc/ansible/playbooks/lamp.yml
[WARNING]: collection community.general does not support Ansible version 2.14.18

PLAY [Installer LAMP sur les serveurs WordPress] *****
TASK [Gathering Facts] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Mettre à jour le cache APT] *****
changed: [client13-site-miel]
TASK [LAMP-COMPLET : Installer les paquets LAMP pour WordPress] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer le module SSL Apache] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer le module Rewrite Apache] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer le module Headers Apache] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer le module Expires Apache] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer le module Apache remoteip] *****
changed: [client13-site-miel]
TASK [LAMP-COMPLET : Créer la configuration Apache remoteip] *****
changed: [client13-site-miel]
TASK [LAMP-COMPLET : Activer la configuration remoteip] *****
changed: [client13-site-miel]
TASK [LAMP-COMPLET : Activer le site SSL par défaut] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer et démarrer Apache] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer et démarrer MariaDB] *****
ok: [client13-site-miel]
TASK [LAMP-COMPLET : Activer et démarrer rsyslog] *****
ok: [client13-site-miel]
RUNNING HANDLER [LAMP-COMPLET : Redémarrer Apache] *****
changed: [client13-site-miel]
PLAY RECAP *****
client13-site-miel : ok=15  changed=5  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0

root@ANSIBLE-SRV-01:/etc/ansible/roles#
```

Exécution réussie : RemoteIP est configuré, le handler Apache est déclenché et failed=0.

Résultat observé : ok=15, changed=5, unreachable=0, failed=0. Le rôle s'est terminé correctement.

6. Vérifier la configuration côté Apache

1. Vérifier que le module remoteip est chargé :

```
apache2ctl -M | grep remoteip
```

Résultat attendu : **remoteip_module (shared)**

2. Vérifier le fichier généré par Ansible :

```
cat /etc/apache2/conf-available/remoteip.conf
```

3. Vérifier que la configuration est activée :

```
ls -l /etc/apache2/conf-enabled/remoteip.conf
```

4. Contrôler la syntaxe Apache :

```
apache2ctl configtest
```

Résultat attendu : **Syntax OK**

5. Surveiller les logs Apache :

```
tail -f /var/log/apache2/access.log
```

Le test doit être fait en accédant au site en passant par Nginx. Si tout est correct, Apache doit afficher l'IP réelle du client au début de chaque ligne de log.

7. Résultat obtenu

Dans les logs ci-dessous, Apache journalise maintenant l'adresse IP réelle du visiteur : **86.195.60.74**. Il ne journalise plus systématiquement l'adresse interne du reverse proxy.

```

86.195.60.74 - - [26/Aug/2026:09:38:44 +0000] "GET / HTTP/1.0" 200 40934 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:45 +0000] "GET /wp-content/plugins/elementor/assets/css/admin-bar.min.css?ver=3.27.2 HTTP/1.0" 200 812 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:45 +0000] "GET /wp-content/uploads/elementor/css/post-17.css?ver=1787652582 HTTP/1.0" 200 750 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:45 +0000] "GET /wp-content/uploads/elementor/css/post-5.css?ver=1787652582 HTTP/1.0" 200 845 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:45 +0000] "GET /wp-content/plugins/elementor/assets/js/elementor-admin-bar.min.js?ver=3.27.2 HTTP/1.0" 200 2770 "https://www. .ovh/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:45 +0000] "GET /wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.9.3 HTTP/1.0" 200 4161 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:46 +0000] "GET /wp-content/uploads/complianz/css/banner-1-optin.css?v=2406 HTTP/1.0" 200 3565 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:46 +0000] "POST /?wc-ajax=get_refreshed_fragments HTTP/1.0" 200 5748 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:46 +0000] "GET /wp-content/uploads/2016/08/8-348x464.png HTTP/1.0" 200 35138 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
86.195.60.74 - - [26/Aug/2026:09:38:46 +0000] "GET /index.php?rest_route=/jetpack/v4/scan HTTP/1.0" 200 987 "https://www. /" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0"
^C
root@SRV-MIEL:~#

```

Logs Apache après configuration : l'adresse IP réelle du client apparaît dans access.log.

Chaîne finale : Client -> Nginx -> X-Forwarded-For -> Apache mod_remoteip -> access.log avec l'IP réelle.

8. Résumé rapide

- Activer mod_remoteip avec community.general.apache2_module.
- Créer /etc/apache2/conf-available/remotep.conf avec les deux IP Nginx de confiance.
- Activer la configuration avec a2enconf remotep.
- Notifier le handler Apache uniquement lorsqu'un changement est détecté.
- Relancer le playbook une seconde fois pour contrôler l'idempotence.
- Vérifier access.log pour confirmer que l'IP réelle est bien journalisée.

Réalisé par
Adel Sadek