TP #2

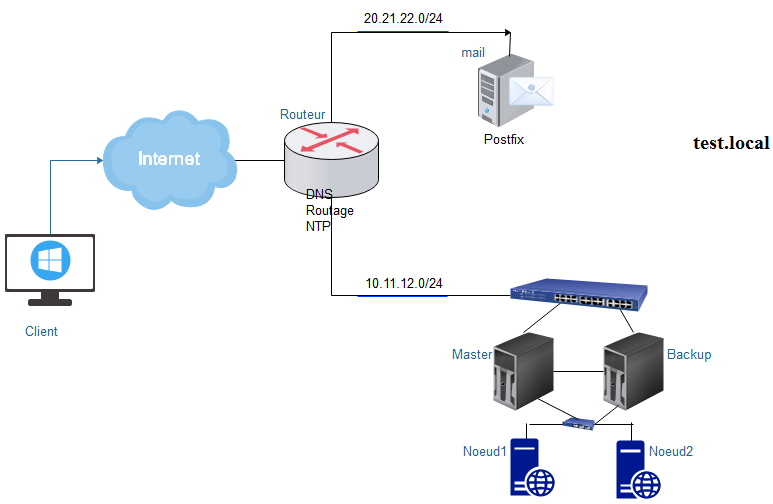


Fig. 1: Topologie de l'entreprise

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Le premier directeur (**master**) | | | Le deuxième directeur (**backup**) | | |
| **Interface** | | **Adresse** | **Interface** | | **Adresse** |
| **NIC1** | | 10.11.12.1/24 | **NIC1** | | 10.11.12.2 /24 |
| **NIC2** | | 192.168.100.1/24 | **NIC2** | | 192.168.100.2/24 |
| **NIC3** | | 172.168.1.1/30 | **NIC3** | | 172.168.1.2/30 |
| **VIP : 10.11.12.99/24** | | | | | |
| **Passerelle virtuelle (VGW) : 192.168.100.99/24** | | | | | |
| Le premier serveur réel (**Noeud1**) | | | Le premier serveur réel (**Noeud2**) | | |
| **Interface** | **Adresse** | | **Interface** | **Adresse** | |
| **NIC1** | 192.168.100.10/24 | | **NIC1** | 192.168.100.20/24 | |
| **Passerelle par défaut : 192.168.100.99/24** | | | | | |

Tableau d’adressage

# **Considération**

Installez les 6 machines de la topologie présentée dans la figure **fig.1** ci-dessus en tenant en considération les spécifications suivantes :

1. Toutes les machines doivent appartenir au domaine DNS: ***test.local***
2. Nommez vos machines selon le schéma ci-dessus : ***Routeur, mail, Master, Backup, Noeud1*** *et* ***Noeud2***.
3. La machine ***Routeur***possède 3 interfaces :

* **La 1ère interface** : attachée au « NAT » de la machine virtuelle.
* **La 2ème interface**: attachée au réseau ***Interne*** (20.21.22.254/24)
* **La 3ème interface**: attachée au réseau ***DMZ*** (10.11.12.254/24)

1. Nous allons mettre en place une solution de haute disponibilité **LVS-NAT** avec **keepalived**. Les interfaces réseaux de vos machines comportent les adresses suivantes : *(voir tableau d’adressage ci-dessus*)

# **Travail demandé**

1. Installez sur le serveur ***Routeur*** les services:
   1. **NTP** : les machines des zones ***Interne*** et ***DMZ***doivent se synchroniser avec **Routeur;**
   2. **DNS :** les machines des réseaux ***Interne*** et ***DMZ***utiliserons ***Routeur*** comme serveur DNS pour résoudre les noms d’hôte. La zone utilisée portera le nom : ***test.local****. (Prévoir plus qu’une zone inversée*).
   3. **Le routage :** il doit être activé sur ***Routeur***, car tous les réseaux de la topologie doivent communiquer entre eux.
   4. Seule le réseau **DMZ** qui doit avoir accès à l’Internet (Prévoir le partage de connexion Internet sur l’interface mise en NAT du **Routeur**)
2. Installez et configurez le service **Postfix** sur le serveur ***mail*.** Créez ensuite deux adresses courriels : **root@test.local** et **user1@test.local**.
3. Installez et configurez le service ***Web*** sur les deux serveurs réels (***Noeud1*** et ***Noeud2***).
4. Installez et configurez ***keepalived*** sur les deux directeurs (**Master** et **Backup**) :
   1. Définissez un script (*avec des codes de retour appropriés*) qui servira de vérificateur de l’état de santé des serveurs réels ***Healthcheker***. (le script permet de vérifier la taille de la RAM disponible sur chacun des serveurs réels. Cette taille doit être supérieure à **50**% de la taille totale de la RAM). la directive ***misc\_dynamic*** doit être présente dans le fichier de configuration.
   2. Spécifiez l’adresse **user1@test.local** pour qu’elle reçoive les informations sur de basculement des répartiteurs de charge.
   3. Spécifiez l’adresse **root@test.local** comme adresse mail d’origine pour les notifications.
   4. Spécifiez le serveur **mail.test.local** comme serveur SMTP pour l’envoi du courrier. (*Le serveur DNS doit être opérationnel avec tous les enregistrements de ressources appropriés*).
   5. Testez la bascule entre (Master/Backup) et entre (Noeud1/Noeud2). Vérifiez ensuite vos tests dans les fichiers journaux dans les serveurs Master et Backup.
   6. Testez la présence de courriel à la suite du basculement.
5. À l’aide de la commande **tcpdump**, capturez le trafic réseau sur l’interfacede l’un des Directeurs. La capture doit être faite durant un basculement et ce, pour pouvoir analyser, par la suite, les paquets du protocoles VRRP.
   1. Utilisez donc la commande :

|  |
| --- |
| **tcpdump -i <interface> -w captureVRRP.pcap** |

* 1. Récupérer le fichier **captureVRRP.pcap** sur votre machine physique et ouvrez-le avec Wireshark et avec un filtre approprié, répondez aux questions suivantes :
     1. L’adresse multicast utilisée ? :

|  |
| --- |
|  |

* + 1. Le champ « protocole » de l'entête IP est positionné à quelle valeur ?

|  |
| --- |
|  |

* + 1. Quelle est l'adresse MAC virtuelle du groupe VRRP ?

|  |
| --- |
|  |

* + 1. En déduire de la question précédente le numéro du groupe VRRP ?

|  |
| --- |
|  |

*Bon courage !!!*