

Spécialité : SSIR-2D

Rapport de Projet de sécurité Réseaux

---

**CONCEPTION ET MISE EN PLACE D'UNE  
ARCHITECTURE SECURISEE DE TEKUP**

---

**Réalisée par :** Wissam nasri

**Encadré par :** Tarek Hdiji

**Année Universitaire :** 2023 – 2024

## Table des matière

### Chapitre1 :conception et mise en place de la solution VPN-MPLS

1.1 Introduction .....	1
1.2 Technologie de Service VPN-MPLS .....	1
1.3 Architecture de la Solution VPN-MPLS .....	1
1.4 Environnement de travail.....	3
1.4.1 GNS3 .....	3
1.4.2 VMware Workstation.....	4
1.4.3 PuTTy.....	4
1.5 Topologie de l'université TEKUP .....	5
1.5.1 Présentation de la topologie .....	5
1.5.2 Adressage de la topologie .....	5
1.6 Mise en place de VPN-MPLS de Tekup .....	8
1.6.1 Configuration de base de l'adressage de chaque Interface .....	8
1.6.2 Configuration des protocoles de routage.....	9
1.6.2.1 Routage OSPF de Backbone IP/MPLS .....	9
1.6.2.2 Configuration de MPLS.....	10
1.6.3 Mise en place des VPN .....	10
1.6.3.1 Configuration de VRF .....	10
1.6.3.2 Configuration les Interfaces et OSPF au niveau CE .....	11
1.6.3.3 Configuration de MP-BGP .....	12
1.7 Validation et test de la connexion.....	13
1.8 Conclusion.....	14

### chapitre2: conception et mise en place de la solution de réseau LAN etendu Tekup

1.1 Introduction .....	15
1.2 Architecture de réseau LAN étendu de Tekup.....	15
1.3 Conception de la Solution LAN .....	16
1.3.1 Vue d'ensemble de l'architecture physiques .....	17
1.3.2 Composants et leurs rôles .....	17
1.3.3 Plan d'adressage .....	18

1.3.4 Protocoles et technologies .....	18
1.4 Description de la Solution Redondante de LAN .....	19
1.5 Environnement de travail.....	20
1.5.1 Environnement logiciel.....	20
1.5.2 Implémentation d'équipement .....	21
1.6 Mise en place de la Solution de LAN Redondante .....	21
1.6.1 Partie Siège .....	21
1.6.1.1 Création de VLAN .....	21
1.6.1.2 Affectation de Port/VLAN au niveau Switch .....	22
1.6.1.3 Configuration Trunk des Switch layer2 et layer3.....	22
1.6.1.4 Configuration Password Console et Password VTY et Password en-.....	24
1.6.1.5 Configuration @IP Management de Switch3.....	25
1.6.1.6 Configuration de Serveur DHCP et Serveur DHCP Backup .....	25
1.6.1.7 Configuration du protocole HSRP au niveau des switch fédérateur 1.....	26
1.6.1.8 Configuration Port Channel.....	27
1.6.1.9 Configuration du routage OSPF sous deux Switch Fédérateurs .....	27
1.6.2 Partie Branch 1 .....	28
1.6.2.1 Création de VLAN .....	28
1.6.2.2 Affectation de Port/VLAN au niveau Switch .....	28
1.6.2.3 Configuration Trunk de Switch SW3 et routeur CE-Branch1 .....	29
1.6.2.4 Configuration du Routage Inter-VLAN au niveau du routeur CE-branch1 ..	29
1.6.2.5 Configuration adresse IP Management de Switch d'accès.....	29
1.6.2.6 Configuration de Serveur DHCP au niveau Router CE-Branch1 .....	30
1.7 Test et Validation des Services de la solution Re-dondante .....	30
1.7.1 Test et validation du service DHCP au niveau des quatreVPCs .....	30
1.7.2 Test et validation du protocole de redondance HSRP .....	31
1.7.3 Test de Connexion entre les pc1,2,3,4.....	31
1.8 Conclusion.....	34
1.1 Introduction .....	35

chapitre3: conception et mise en place de la solution de monotoring et sécurité AAA

1.2.2 Critères de choix des solutions de supervision .....	36
1.2.3 Solution proposé .....	38
1.3 Model de fonctionnement de la Solution Moni-toring nagios .....	39
1.3.1 Fonctionnement.....	39
1.3.2 Architecture de nagios .....	40
1.3.3 L'interface utilisée par Nagios .....	40
1.3.4 Le langage de programmation (ou serveur d'application).....	41
1.3.5 Le serveur de bases de données MySQL.....	41
1.3.6 . Le greffon .....	42
1.3.7 Les principaux plugins .....	43
1.4 Mise en place de la Solution Monitoring.....	44
1.4.1 L'architecture de la solution monitoring .....	44
1.4.2 Installer et configurer Nagios Core .....	44
1.9 conclusion .....	57

## Table de figure

Figure 1: Architecture de la Solution VPN-MPLS.....	3
Figure 2:Logo GNS3 .....	4
Figure 3:Logo VMware Workstation Pro .....	4
Figure 4:Logo PuTTY .....	5
Figure 5:Topologie de l'université TEKUP .....	6
Figure 6:Configuration de l'adressage de chaque Interface de PE1 .....	9
Figure 7:Configuration de l'adressage de chaque Interface de PE1 .....	9
Figure 8:configuration de MPLS et PE1 .....	10
Figure 9:Création du VRF de PE1 .....	11
Figure 10:Activation du VRF de PE1.....	11
Figure 11:Configuration des Interfaces et OSPF au niveau CE11 .....	12
Figure 12:Configuration de MP-BGP au niveau PE1 .....	13
Figure 13: Vérification de la connexion entre customer 11 et 12 .....	13
Figure 14:Vérification de la connexion entre customer 21 et 22.....	13
Figure 15:Architecture de réseau LAN étendu de Tekup .....	16
Figure 16:Les composants de l'architecture de réseau LAN étendu de Tekup .....	18
Figure 17:plan d'addressage des VLANs .....	18
Figure 18:logo de putty .....	20
Figure 19:logo de VMware Workstation Pro .....	20
Figure 20:logo de gns3 .....	21
Figure 21:logo du commutateur .....	21
Figure 22:logo du routeur .....	21
Figure 23:creation de vlan .....	22
Figure 24:Affectation de Port/VLAN au niveau Switch.....	22
Figure 25:port trunk au niveau de switch1 .....	23
Figure 26:port trunk au niveau de federateur1 .....	23
Figure 27:port trunk au niveau de federateur1 .....	24
Figure 28:Config Password Console et vty .....	25
Figure 29:Config @IP Management de Switch3 .....	25
Figure 30:Configuration de Serveur DHCP .....	26
Figure 31:Configuration du protocole HSRP .....	27
Figure 32:Configuration Port Channel .....	27
Figure 33:Configuration du routage OSPF.....	28
Figure 34:Création de VLAN .....	28
Figure 35:Affectation de Port/VLAN au niveau Switch3.....	28
Figure 36:Config Trunk de Switch SW3 .....	29
Figure 37:Config du Routage Inter-VLAN .....	29

Figure 38:Config adresse IP Management .....	30
Figure 39:Configuration de Serveur DHCP.....	30
Figure 40:ip dhcp pc1 .....	30
Figure 41:ip dhcp pc2 .....	30
Figure 42:ip dhcp pc3 .....	31
Figure 43:ip dhcp pc4 .....	31
Figure 44:test hsrp.....	31
Figure 45:test hsrp.....	31
Figure 46:architecture standard de nagios .....	40
Figure 47:architecture sécurisée .....	44

---

# CHAPITRE 1

---

## 1.1 Introduction

Dans ce premier chapitre, nous commencerons par présenter la technologie de Service VPN-MPLS ainsi que l'architecture de la solution VPN-MPLS. Ensuite, Nous aborderons également l'environnement de travail nécessaire pour mettre en place et tester ces services, en utilisant des outils tels que GNS3, VirtualBox et VMware puis, nous examinerons la topologie spécifique de l'université TEKUP et exposons le processus de mise en place d'un VPN-MPLS. Enfin, nous détaillons des étapes de validation et de test de la connexion pour assurer son bon fonctionnement.

## 1.2 Technologie de Service VPN-MPLS

La technologie de Service VPN-MPLS, ou Virtual Private Network - Multi-Protocol Label Switching, est une méthode de réseau privé virtuel qui combine les avantages des réseaux privés traditionnels avec la flexibilité et l'efficacité du commutateur d'étiquettes multiprotocole (MPLS). En utilisant des étiquettes pour acheminer les données à travers le réseau, le VPN-MPLS permet de créer des connexions sécurisées entre des sites distants sur un réseau étendu. Cette technologie offre une qualité de service garantie, une gestion efficace du trafic et la possibilité d'intégrer différents types de protocoles de communication, ce qui en fait une solution populaire pour les entreprises ayant des besoins de connectivité complexe et sécurisée.

## 1.3 Architecture de la Solution VPN-MPLS

L'architecture de la solution VPN-MPLS comprend plusieurs composants essentiels qui travaillent ensemble pour fournir des services de réseau privé virtuel sécurisés et efficaces.

Voici les principaux éléments de cette architecture :

- Provider Edge (PE) Router : Ces routeurs sont situés aux bords du réseau MPLS et servent de points d'entrée et de sortie pour les connexions VPN-MPLS. Ils sont responsables de l'encapsulation et du désencapsulation des données VPN, ainsi que de la distribution des étiquettes MPLS.
- Customer Edge (CE) Router : Ces routeurs sont situés aux bords du réseau client et sont connectés aux PE routers. Ils jouent un rôle crucial dans l'établissement et la gestion des connexions VPN-MPLS avec les PE routers.
- Provider (P) Router : Ces routeurs sont situés au sein du réseau MPLS et servent à acheminer les paquets de données en fonction des étiquettes MPLS. Ils assurent la commutation rapide et efficace du trafic entre les PE routers.
- Virtual Routing and Forwarding (VRF) Tables : Chaque connexion VPN-MPLS est associée à une table VRF dédiée, qui permet d'isoler le trafic entre différents clients ou réseaux virtuels. Cette segmentation garantit la confidentialité et la sécurité des données transitant sur le réseau VPN-MPLS.
- Label Distribution Protocol (LDP) : Ce protocole est utilisé pour distribuer les étiquettes MPLS entre les routeurs MPLS afin d'établir des chemins de communication virtuels dans le réseau. Il permet également aux routeurs de synchroniser leurs tables de commutation MPLS.
- Label Edge Router (LER) : Le LER est le point d'entrée du réseau MPLS. Il est responsable de l'ajout et du retrait des étiquettes MPLS aux paquets de données lorsqu'ils entrent ou sortent du réseau MPLS. Le LER marque les paquets de données avec des étiquettes appropriées en fonction des politiques de routage définies.
- Label Switching Router (LSR) : Les LSRs sont les nœuds de transit du réseau MPLS. Ils sont chargés de commuter les paquets de données en fonction des étiquettes MPLS associées à chaque paquet. Les LSRs utilisent des tables de commutation pour prendre

des décisions sur la transmission des paquets en se basant sur les étiquettes MPLS.

- Label Switched Path (LSP) : Un LSP est un chemin préétabli à travers le réseau MPLS le long duquel les paquets de données sont transmis. Les LSPs sont établis dynamiquement à l'aide de protocoles de signalisation MPLS tels que RSVP-TE (Resource Reservation Protocol - Traffic Engineering) ou LDP (Label Distribution Protocol). Une fois qu'un LSP est établi, les paquets de données suivent ce chemin spécifique à travers le réseau.

Ensemble, ces composants forment une architecture robuste et évolutive qui permet la création et la gestion efficace de réseaux privés virtuels à l'aide de la technologie VPN-MPLS comme le montre la figure suivante :

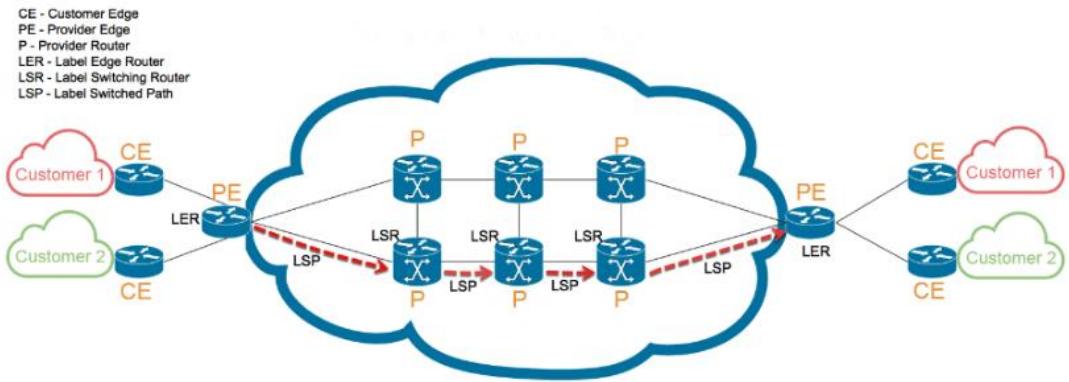


Figure 1: Architecture de la Solution VPN-MPLS

## 1.4 Environnement de travail

Nous allons maintenant présenter les logiciels utilisés dans notre projet à savoir :

GNS3, VMware et putty.

### 1.4.1 GNS3

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.



Figure 2:Logo GNS3

#### 1.4.2 VMware Workstation

VMware Workstation Pro : est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels



Figure 3:Logo VMware Workstation Pro

#### 1.4.3 PuTTY

PUTTY : est un client SSH open-source populaire, utilisé pour l'accès aux machines virtuelles à partir de la machine hôte sous Windows. Avec ce logiciel, vous pouvez travailler, depuis votre ordinateur personnel, sur une machine Linux du DMS, en mode ligne de commandes.

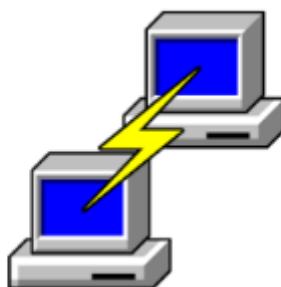


Figure 4:Logo PuTTY

## 1.5 Topologie de l'université TEKUP

### 1.5.1 Présentation de la topologie

La figure 1.5 présente l'architecture élaborée dans le simulateur GNS3 pour présenter la Topologie de l'université TEKUP.

### 1.5.2 Adressage de la topologie

Dans cette section, nous nous intéressons à la définition d'un plan d'adressage qui nous

permet d'interconnecter les différentes zones dans l'architecture.

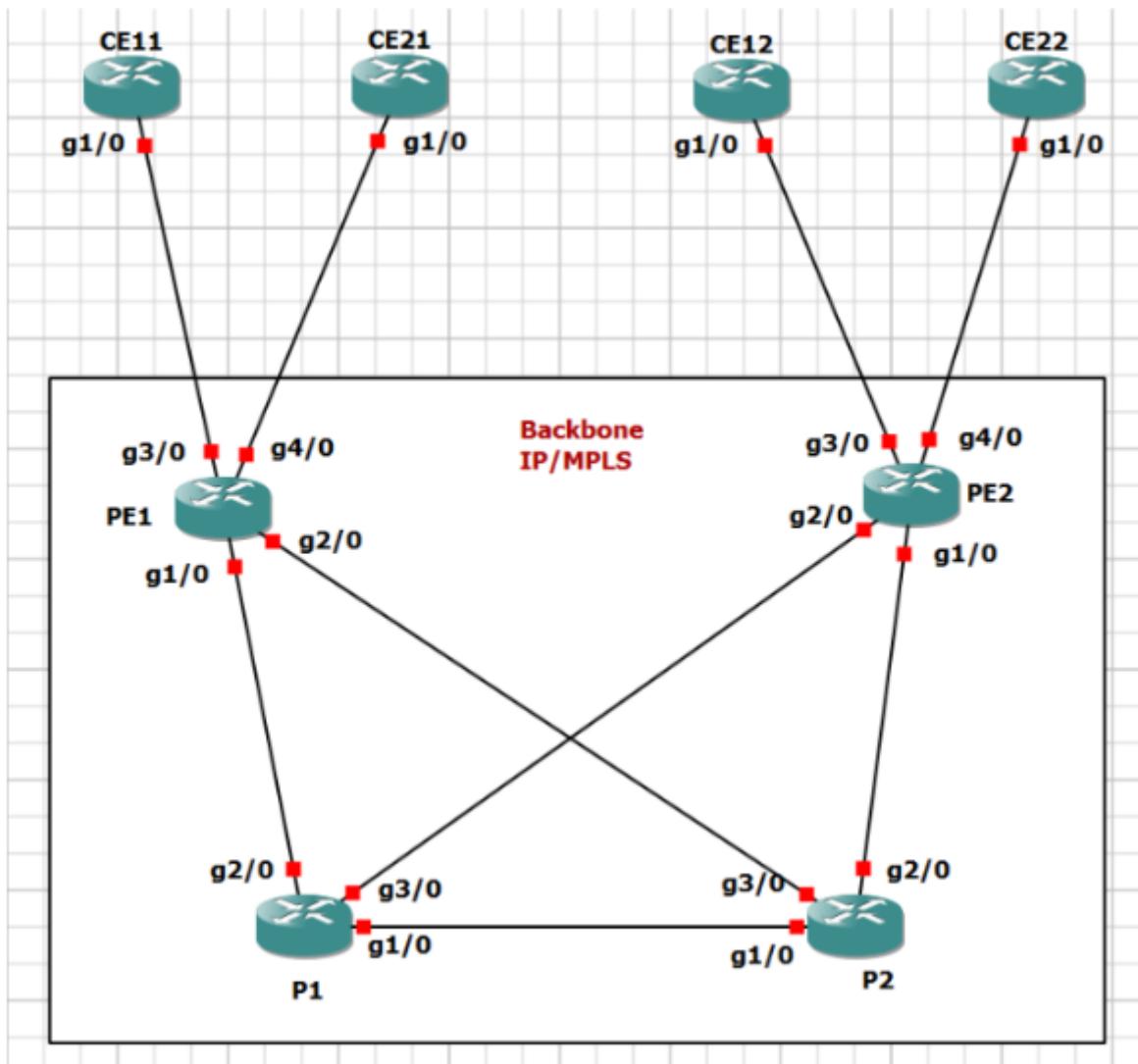


Figure 5:Topologie de l'université TEKUP

	<b>Interface</b>	<b>Adresse IP</b>
<b>CE11</b>	G1/0 Connect to PE1	192.168.1.2/30
	Loopback0	172.16.11.11/32
<b>CE12</b>	G1/0 Connect to PE2	192.168.1.10/30
	Loopback0	172.16.12.12/32
<b>CE21</b>	G1/0 Connect to PE1	192.168.1.6/30
	Loopback0	172.16.21.21/32
<b>CE22</b>	G1/0 Connect to PE2	192.168.1.14/30
	Loopback0	172.16.22.22/32
<b>PE1</b>	Loopback0	1.1.1.1/32
	G1/0 Connect to P1	10.1.1.1/30
	G2/0 Connect to P2	10.1.1.5/30
	G3/0 Connect to CE11	192.168.1.1/30
	G4/0 Connect to CE21	192.168.1.5/30
<b>PE2</b>	Loopback0	2.2.2.2/32

	G1/0 Connect to P2	10.1.1.9/30
	G2/0 Connect to P1	10.1.1.13/30
	G3/0 Connect to CE12	192.168.1.9/30
	G4/0 Connect to CE22	192.168.1.13/30
<b>P1</b>	Loopback0	3.3.3.3/32
	G1/0 connect to P2	10.1.1.21/30
	G2/0 connect to PE1	10.1.1.2/30
	G3/0 connect to PE2	10.1.1.14/30
<b>P2</b>	Loopback0	4.4.4.4/32
	G1/0 connect to P1	10.1.1.22/30
	G2/0 connect to PE2	10.1.1.10/30
	G3/0 connect to PE1	10.1.1.6/30

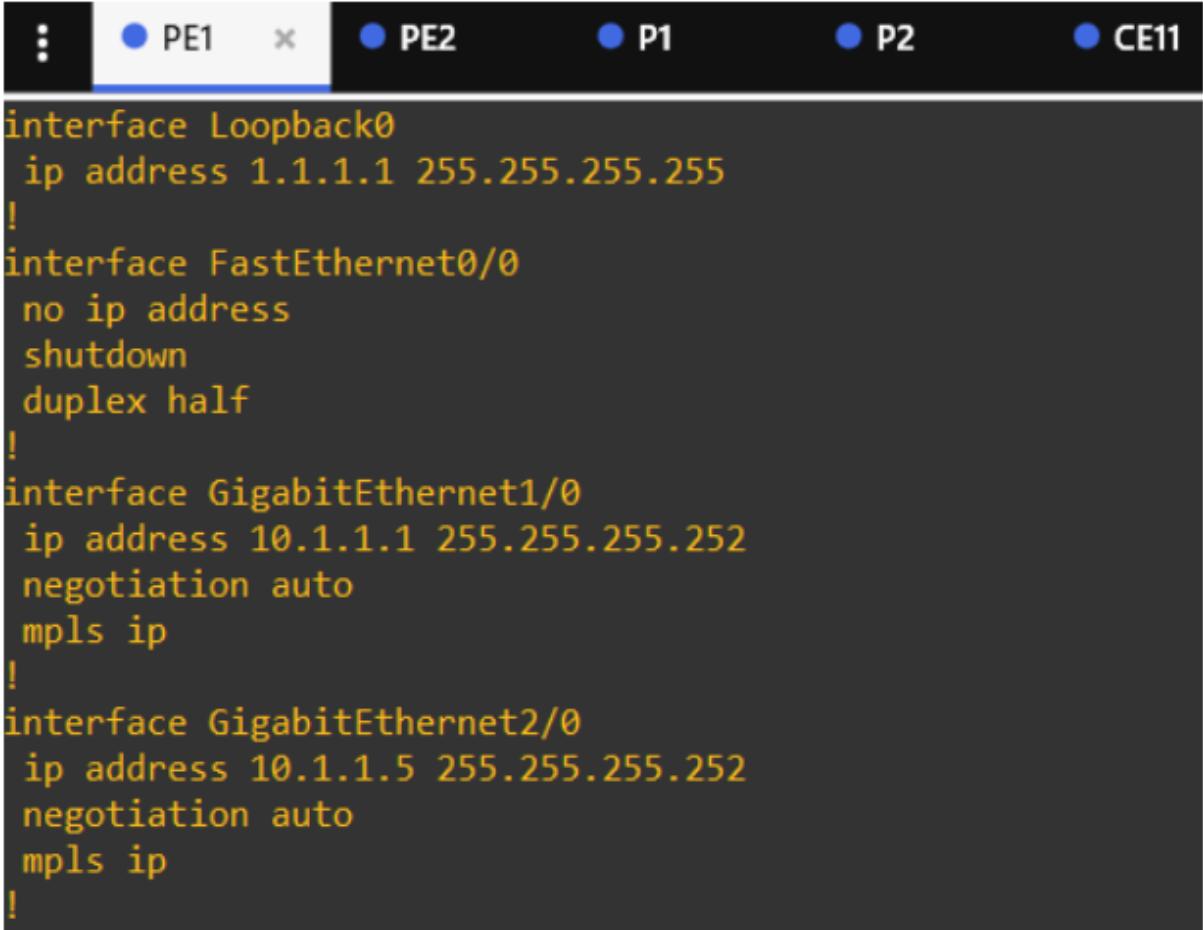
## 1.6 Mise en place de VPN-MPLS de Tekup

### 1.6.1 Configuration de base de l'adressage de chaque Interface

Dans une première étape, nous devons configurer les différentes interfaces des routeurs

à utiliser. Ci-dessous, un exemple de configuration de quelques interfaces du routeur PE1

est illustré.



```
PE1 PE2 P1 P2 CE11

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 10.1.1.1 255.255.255.252
 negotiation auto
 mpls ip
!
interface GigabitEthernet2/0
 ip address 10.1.1.5 255.255.255.252
 negotiation auto
 mpls ip
!
```

Figure 6: Configuration de l'adressage de chaque Interface de PE1

### 1.6.2 Configuration des protocoles de routage

#### 1.6.2.1 Routage OSPF de Backbone IP/MPLS

Nous appliquerons le protocole OSPF sur tous les routeurs du Backbone IP/MPLS tout en prenant en considération Area 0.

Nous donnerons un exemple de configuration ci-dessous le routeur PE1

```
!
router ospf 1
 network 1.1.1.1 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.4 0.0.0.3 area 0
!
```

Figure 7: Configuration de l'adressage de chaque Interface de PE1

### 1.6.2.2 Configuration de MPLS

La technologie MPLS fonctionne par commutation des labels. Ainsi, il est obligatoire d'activer le protocole MPLS sur les routeurs du Backbone tout en prenant en considération

les paramètres exigés. Pour ce faire, nous procédonss comme il est noté ci-dessous (Exemple

de configuration PE1) en tapant les dites commandes sur toutes les routeurs appartenant

au Backbone MPLS/IP

```
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
mpls label protocol ldp
!
```

```
!
interface GigabitEthernet1/0
  ip address 10.1.1.1 255.255.255.252
  negotiation auto
  mpls ip
!
interface GigabitEthernet2/0
  ip address 10.1.1.5 255.255.255.252
  negotiation auto
  mpls ip
!
```

Figure 8:configuration de MPLS et PE1

### 1.6.3 Mise en place des VPN

#### 1.6.3.1 Configuration de VRF

- Création et Activation du VRF

```
!
ip vrf VPN_Customer1
rd 100:1
route-target export 100:1
route-target import 100:1
!
ip vrf VPN_Customer2
rd 100:2
route-target export 100:2
route-target import 100:2
!
```

Figure 9:Création du VRF de PE1

```
!
interface GigabitEthernet3/0
ip vrf forwarding VPN_Customer1
ip address 192.168.1.1 255.255.255.252
negotiation auto
!
interface GigabitEthernet4/0
ip vrf forwarding VPN_Customer2
ip address 192.168.1.5 255.255.255.252
negotiation auto
!
```

Figure 10:Activation du VRF de PE1

#### 1.6.3.2 Configuration les Interfaces et OSPF au niveau CE

Nous appliquerons le protocole OSPF sur tous les routeurs du CEij tout en prenant

en considération Area ij.

```
!
interface Loopback0
 ip address 172.16.11.11 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 192.168.1.2 255.255.255.252
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 network 172.16.11.11 0.0.0.0 area 11
 network 192.168.1.0 0.0.0.3 area 11
!
```

Figure 11: Configuration des Interfaces et OSPF au niveau CE11

#### 1.6.3.3 Configuration de MP-BGP

Pour que le VRF fonctionne, nous distribuons le chemin vers tout le réseau. Les commandes ci-dessous seront exécutées sur PE1 ayant les interfaces sur laquelle est attaché le VRF.

```

!
router bgp 100
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 update-source Loopback0
!
  address-family ipv4
    exit-address-family
!
  address-family vpnv4
    neighbor 2.2.2.2 activate
    neighbor 2.2.2.2 send-community both
    exit-address-family
!
  address-family ipv4 vrf VPN_Customer1
    redistribute ospf 100
    exit-address-family
!
  address-family ipv4 vrf VPN_Customer2
    redistribute ospf 200
    exit-address-family
!

```

Figure 12:Configuration de MP-BGP au niveau PE1

## 1.7 Validation et test de la connexion

Pour vérifier la connexion entre les différents sites de clients, nous tapons la commande

suivante au niveau CEij :

```

CE11#ping 172.16.12.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/118/128 ms
CE11#

```

Figure 13: Vérification de la connexion entre customer 11 et 12

```

CE21#ping 172.16.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/148/240 ms
CE21#

```

Figure 14:Vérification de la connexion entre customer 21 et 22

## 1.8 Conclusion

Dans ce chapitre, nous avons présenté la technologie de Service VPN-MPLS. Ensuite nous avons détaillé l'implémentation de l'architecture sur l'environnement virtuel GNS3 puis nous avons exposé la Topologie de l'université TEKUP et nous avons fini par Valider et tester la connexion pour assurer le bon fonctionnement du service VPN-MPLS.

---

# CHAPITRE 2

---

## 1.1 Introduction

Ce deuxième chapitre est consacré à l'implémentation et la configuration de notre architecture réseau. En premier lieu, nous commençons par la présentation d'architecture de réseau LAN étendu de Tekup. Ensuite, nous clarifions la conception architecturale de la solution LAN que nous allons suivre dans la partie réalisation de notre projet. Nous détaillons ainsi la description de la solution redondante de LAN. Par la suite, nous exposons l'environnement de travail. Puis, nous passerons à la mise en place de la solution de LAN redondante et nous clôturons par des test et validation des services de notre solution.

## 1.2 Architecture de réseau LAN étendu de Tekup

L'architecture de réseau LAN étendu de Tekup est conçue pour connecter de manière transparente les différents sites de l'organisation, en permettant une communication fluide et sécurisée entre eux. À travers des connexions WAN efficaces, les sites distants sont interconnectés, créant ainsi un réseau uniifié.

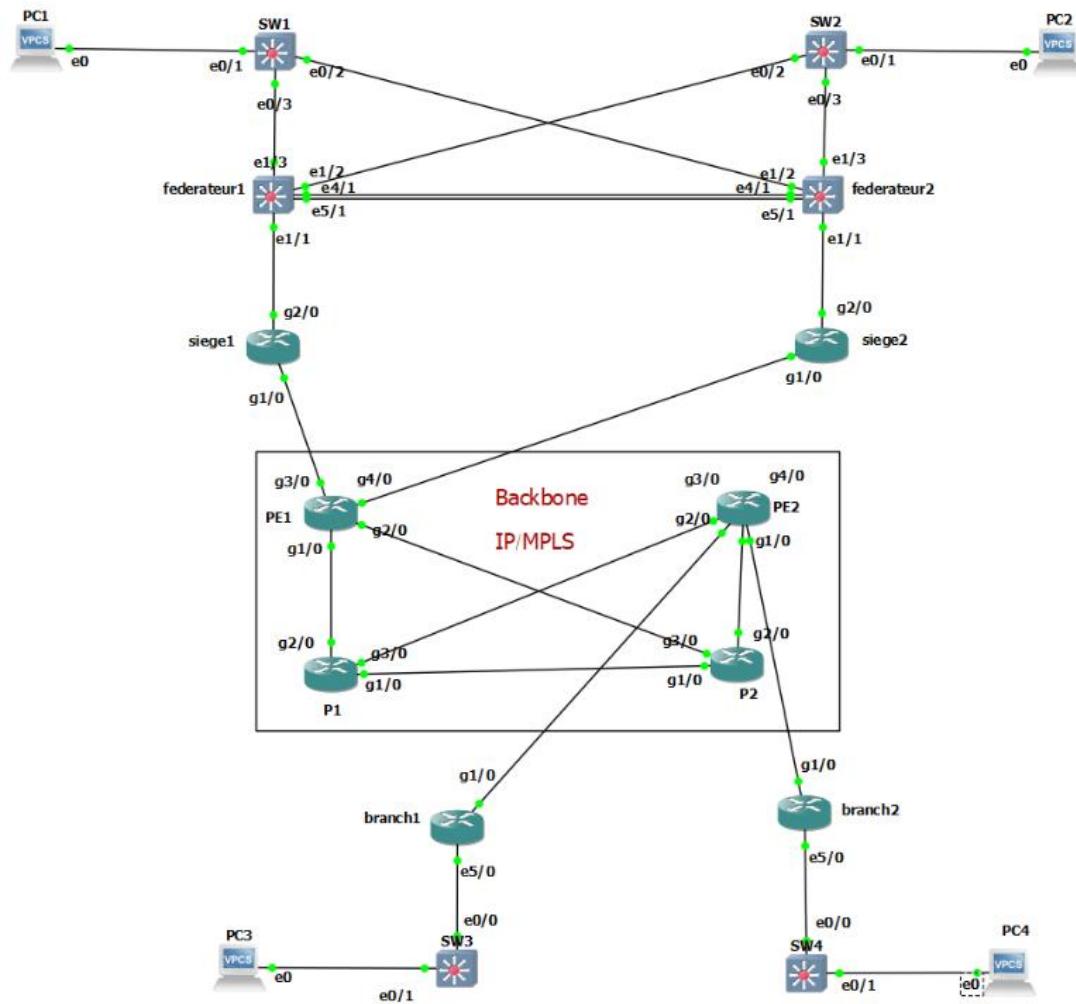


Figure 15: Architecture de réseau LAN étendu de Tekup

Pour garantir la résilience et la disponibilité du réseau, des mesures de redondance sont

mises en place. Cela peut inclure des liens WAN redondants, des routeurs redondants et

des commutateurs redondants, permettant ainsi une continuité des opérations même en

cas de panne d'un équipement ou d'une connexion.

### 1.3 Conception de la Solution LAN

La conception de la solution LAN fait référence à la planification et à la définition des éléments techniques et fonctionnels qui composent le réseau local (LAN) de chaque site

distant.

### 1.3.1 Vue d'ensemble de l'architecture physiques

Le réseau est divisé en plusieurs segments, chacun connecté à un commutateur différent

(SW1 ou SW2). Cette segmentation permet d'isoler le trafic de diffusion et d'optimiser les performances du réseau en limitant le nombre de périphériques pouvant communiquer

directement entre eux.

Les périphériques Fédérateur (Fédérateur1 et Fédérateur2) sont connectés aux commutateurs ce qui suggère qu'ils fonctionnent à un niveau supérieur dans la hiérarchie du

réseau. Cela pourrait indiquer qu'ils fournissent des services de routage, de DHCP ou d'autres services réseau entre les différents segments et le réseau plus large.

La présence de deux périphériques Fédérateur (Fédérateur1 et Fédérateur2) pourrait indiquer des mesures de redondance, garantissant la continuité du fonctionnement du réseau en cas de défaillance d'un périphérique.

Les connexions entre les périphériques Fédérateur suggèrent un chemin redondant pour

le flux de données, offrant des routes alternatives en cas de défaillance de liaisons.

### 1.3.2 Composants et leurs rôles

Dans ce projet, nous avons commencé par la création de notre topologie réseau. Puis nous avons fait la configuration réseau pour assurer la communication les équipements utilisées. Les équipements réseau utilisées sont présentés dans le tableau suivant :

Equipement	Marque	Application ou Fonctionnalité	Nombre
Switch niveau 2	Cisco IOU L2	Connectent plusieurs périphériques au sein d'un même segment de réseau	4
Switch niveau 3	Cisco IOU L2	Présentent divers composants réseau : routeurs, serveurs DHCP	2
Routeur	C7200V15	Routage Inter-VLAN	4
VPC	-	Périphériques d'utilisateurs finaux	4

Figure 16:Les composants de l'architecture de réseau LAN étendu de Tekup

### 1.3.3 Plan d'adressage

Dans cette section, nous nous intéressons à la définition d'un plan d'adressage qui nous permet d'interconnecter les différentes zones dans l'architecture. Le tableau suivant présente l'adressage des VLANs

Nom partie	Vlan Name	Vlan ID	Adresse réseau	Masque	Passerelle
Siège	DATA1	10	172.16.10.0/24	255.255.255.0 (/24)	172.16.10.1
	DATA2	15	172.16.15.0/24	255.255.255.0 (/24)	172.16.15.1
	Management	20	172.16.20.0/24	255.255.255.0 (/24)	172.16.20.1
Branch1	Management	101	172.16.101.0/24	255.255.255.0 (/24)	172.16.101.1
	DATA	102	172.16.102.0/24	255.255.255.0 (/24)	172.16.102.1
Branch2	Management	103	172.16.103.0/24	255.255.255.0 (/24)	172.16.103.1
	DATA	104	172.16.104.0/24	255.255.255.0 (/24)	172.16.104.1

Figure 17:plan d'addressage des VLANs

### 1.3.4 Protocoles et technologies

- DHCP : Le protocole DHCP (Dynamic Host Configuration Protocol) est un standard TCP/IP conçu pour simplifier les gestions de la configuration d'IP hôte. DHCP permet d'utiliser des serveurs pour affecter dynamiquement des adresses IP et d'autre paramètres de configuration correspondante pour les clients DHCP de votre réseau.
- EtherChannel : EtherChannel (port Channel) est une technologie de groupage de liaisons principalement utilisée sur les commutateurs Cisco. Son objectif est d'augmenter la vitesse et la tolérance aux pannes entre les serveurs, les switches et les routeurs.

- HSRP : Le protocole HSRP ou Hot Standby Routing Protocol, est un protocole propriétaire Cisco. HSRP permet d'augmenter la tolérance de panne sur un réseau en créant un routeur virtuel à partir de 2 routeurs physiques (ou plus), une élection déterminera le routeur actif et les autres routeurs seront en « attente » (standby).

## 1.4 Description de la Solution Redondante de LAN

La redondance en réseau LAN (Local Area Network) est une conception de systèmes qui consiste à dupliquer un composant pour disposer d'une solution de secours en cas de

défaillance. Elle est utilisée pour augmenter la fiabilité du système, assurer une disponibilité élevée et protéger contre les pertes et les pannes dans un environnement réseau.

Elle vise à minimiser les interruptions de service en cas de défaillance d'un composant ou

d'un lien dans le réseau, tout en assurant une connectivité continue pour les utilisateurs.

La redondance peut être mise en œuvre à différents niveaux, tels que matériel, logiciel, informations et temps, et peut prendre la forme de matériel redondant, de logiciels redondants, de données redondantes et de temps redondant. En réseau LAN, la redondance

est souvent utilisée pour améliorer la fiabilité du système et garantir une connectivité continue en cas de défaillance d'un composant.

L'objectif d'une solution redondante de LAN est de minimiser les temps d'arrêt du réseau et d'assurer la continuité des opérations. Cela peut être particulièrement important

dans les environnements où la disponibilité du réseau est essentielle.

En mettant en œuvre une solution redondante de LAN, les organisations peuvent améliorer la fiabilité de leur réseau, réduire les interruptions de service et garantir une

connectivité continue pour leurs utilisateurs et leurs services.

## 1.5 Environnement de travail

Dans cette partie, nous allons présenter notre environnement matériel et logiciel utilisé pour réaliser notre solution en introduisant les différents choix technologiques faits pour venir à bout de ce travail.

### 1.5.1 Environnement logiciel

Durant ce projet, on a exploité les outils logiciels et les technologies suivantes :

-PuTTY : est un client SSH open-source populaire, utilisé pour l'accès aux machines virtuelles à partir de la machine hôte sous Windows. Avec ce logiciel, vous pouvez travailler, depuis votre ordinateur personnel, sur une machine Linux du DMS, en mode ligne de commandes.



Figure 18:logo de putty

-VMware Workstation Pro : est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels



Figure 19:logo de VMware Workstation Pro

GNS3 : GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émutation ou la simulation de réseaux informatiques.



Figure 20:logo de gns3

### 1.5.2 Implémentation d'équipement

- Commutateur : nous avons utilisées l'image Cisco IOU L2



Figure 21:logo du commutateur

- Routeur : nous avons utilisées l'image C7200V15



Figure 22:logo du routeur

## 1.6 Mise en place de la Solution de LAN Redondante

### 1.6.1 Partie Siège

#### 1.6.1.1 Création de VLAN

Dans une première étape, nous avons créés les VLANs 10,15,20 et 30 au niveau des

switch layer 2 et layer 3. Ci-dessous, un exemple de configuration dans le switch fédéral. Le switch fédéral est illustré

VLAN Name	Status	Ports
1 default	active	Et0/0, Et0/1, Et0/2, Et0/3 Et1/0, Et1/1, Et2/0, Et2/1 Et2/2, Et2/3, Et3/0, Et3/1 Et3/2, Et3/3, Et4/0, Et4/2 Et4/3, Et5/0, Et5/2, Et5/3 Et6/0, Et6/1, Et6/2, Et6/3 Et7/0, Et7/1, Et7/2, Et7/3 Et8/0, Et8/1, Et8/2, Et8/3 Et9/0, Et9/1, Et9/2, Et9/3
10 Data1	active	
15 Data2	active	
20 Management	active	
30 VLAN30	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figure 23:creation de vlan

#### 1.6.1.2 Affectation de Port/VLAN au niveau Switch

Nous avons configuré les différentes interfaces des switches à utiliser. Ci-dessous, un

exemple de configuration de quelques interfaces du switch1 est illustré

```
!
interface Ethernet0/1
  switchport access vlan 10
  switchport mode access
!
```

Figure 24:Affectation de Port/VLAN au niveau Switch

#### 1.6.1.3 Configuration Trunk des Switch layer2 et layer3

La figure suivante illustre la configuration du Trunk au niveau des Switch layer2 et layer3

```
!
interface Ethernet0/2
switchport trunk allowed vlan 1,10,15,20,1002-1005
switchport trunk encapsulation dot1q
switchport trunk native vlan 20
switchport mode trunk
!
interface Ethernet0/3
switchport trunk allowed vlan 1,10,15,20,1002-1005
switchport trunk encapsulation dot1q
switchport trunk native vlan 20
switchport mode trunk
!
```

Figure 25:port trunk au niveau de switch1

```
!
interface Ethernet1/2
switchport trunk allowed vlan 1,10,15,20,1002-1005
switchport trunk encapsulation dot1q
switchport trunk native vlan 20
switchport mode trunk
!
interface Ethernet1/3
switchport trunk allowed vlan 1,10,15,20,1002-1005
switchport trunk encapsulation dot1q
switchport trunk native vlan 20
switchport mode trunk
!
```

Figure 26:port trunk au niveau de federateur1

```
!
interface Ethernet4/1
switchport trunk allowed vlan 1,10,15,20,30,1002-1005
switchport trunk encapsulation dot1q
switchport trunk native vlan 20
switchport mode trunk
channel-group 1 mode on
!
interface Ethernet4/2
!
interface Ethernet4/3
!
interface Ethernet5/0
!
interface Ethernet5/1
switchport trunk allowed vlan 1,10,15,20,30,1002-1005
switchport trunk encapsulation dot1q
switchport trunk native vlan 20
switchport mode trunk
channel-group 1 mode on
!
```

Figure 27:port trunk au niveau de federateur1

#### 1.6.1.4 Configuration Password Console et Password VTY et Password enable au niveau de tous les équipements

La figure suivante illustre la configuration du password enable, console et vty

```
line con 0
  exec-timeout 0 0
  privilege level 15
  password asma
  logging synchronous
  login local
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  password asma
  login local
!
!
end
```

Figure 28:Config Password Console et vty

#### 1.6.1.5 Configuration @IP Management de Switch3

Nous avons créés l'adresse IP management du VLAN20 au niveau des switch layer 2.

Ci-dessous, un exemple de configuration dans le switch1 est illustré

```
!
interface Vlan20
  ip address 172.16.20.101 255.255.255.0
!
ip default-gateway 172.16.20.1
ip forward-protocol nd
!
```

Figure 29:Config @IP Management de Switch3

#### 1.6.1.6 Configuration de Serveur DHCP et Serveur DHCP Backup

La figure suivante illustre la configuration du serveur DHCP au niveau de deux Fé-

dérateurs 1 et 2 pour les deux VLAN 10 et 15 tel que les 10 premiers @IP sont réservés pour chaque VLAN.

```
!
ip dhcp excluded-address 172.16.10.1 172.16.10.10
ip dhcp excluded-address 172.16.15.1 172.16.15.10
!
ip dhcp pool Data1
  network 172.16.10.0 255.255.255.0
  default-router 172.16.10.1
  dns-server 8.8.8.8
!
ip dhcp pool Date2
  network 172.16.15.0 255.255.255.0
  default-router 172.16.15.1
  dns-server 8.8.8.8
!
```

Figure 30:Configuration de Serveur DHCP

#### 1.6.1.7 Configuration du protocole HSRP au niveau des switch fédérateur 1 et 2

La figure suivante illustre la configuration du HSRP au niveau des switch fédérateur1

```

interface Vlan10
  ip address 172.16.10.2 255.255.255.0
  standby 10 ip 172.16.10.1
  standby 10 priority 120
  standby 10 preempt
!
interface Vlan15
  ip address 172.16.15.2 255.255.255.0
  standby 15 ip 172.16.15.1
  standby 15 priority 120
  standby 15 preempt
!
interface Vlan20
  ip address 172.16.20.2 255.255.255.0
  standby 20 ip 172.16.20.1
  standby 20 priority 120
  standby 20 preempt
!
interface Vlan30
  ip address 192.168.1.45 255.255.255.252
  ip ospf cost 3000
!
```

Figure 31:Configuration du protocole HSRP

#### 1.6.1.8 Configuration Port Channel

Nous avons créés le port channel au niveau des switch layer 3. Ci-dessous, un exemple

de configuration dans le switch federateur1 est illustré

```

.
interface Port-channel1
  switchport trunk allowed vlan 1,10,15,20,30,1002-1005
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 20
  switchport mode trunk
```

Figure 32:Configuration Port Channel

#### 1.6.1.9 Configuration du routage OSPF sous deux Switch Fédérateurs

La figure suivante illustre la configuration du routage OSPF au niveau des switch fédérateur1

```

router ospf 100
  router-id 10.10.10.10
  passive-interface default
  no passive-interface Ethernet1/1
  no passive-interface Vlan30
  network 172.16.10.0 0.0.0.255 area 11
  network 172.16.15.0 0.0.0.255 area 11
  network 172.16.20.0 0.0.0.255 area 11
  network 192.168.1.44 0.0.0.3 area 11
!
```

Figure 33:Configuration du routage OSPF

## 1.6.2 Partie Branch 1

### 1.6.2.1 Crédation de VLAN

Dans une première étape, nous avons créés les VLANs 101,102 au niveau des switch

layer 2 et layer 3. Ci-dessous, un exemple de configuration dans le switch3 est illustré

```

SW3#show vlan brief

VLAN Name          Status    Ports
----- -----
1     default       active    Et0/2, Et0/3, Et1/0, Et1/1
                      Et1/2, Et1/3, Et2/0, Et2/1
                      Et2/2, Et2/3, Et3/0, Et3/1
                      Et3/2, Et3/3
101   Management   active
102   Data          active    Et0/1
1002  fddi-default act/unsup
1003  token-ring-default act/unsup
1004  fddinet-default act/unsup
1005  trnet-default act/unsup
SW3#
```

Figure 34:Création de VLAN

### 1.6.2.2 Affectation de Port/VLAN au niveau Switch

La figure suivante illustre la configuration de l'interface du switch3

```

!
interface Ethernet0/1
  switchport access vlan 102
  switchport mode access
!
```

Figure 35:Affectation de Port/VLAN au niveau Switch3

#### 1.6.2.3 Configuration Trunk de Switch SW3 et routeur CE-Branch1

Nous avons configuré les différentes interfaces des switches et routeur à utiliser.

Ci-

dessous, un exemple de configuration de quelques interfaces du switch

```
!
interface Ethernet0/0
switchport trunk allowed vlan 101,102
switchport trunk encapsulation dot1q
switchport trunk native vlan 101
switchport mode trunk
!
```

Figure 36:Config Trunk de Switch SW3

#### 1.6.2.4 Configuration du Routage Inter-VLAN au niveau du routeur CE-branch1

Nous avons configuré les deux Subinterface au niveau Router CE-branch1 à utiliser.

Ci-dessous, un exemple de configuration des interfaces du routeur branch1 est illustré

```
!
interface Ethernet5/0
no ip address
duplex half
!
interface Ethernet5/0.101
encapsulation dot1Q 101 native
ip address 172.16.101.1 255.255.255.0
!
interface Ethernet5/0.102
encapsulation dot1Q 102
ip address 172.16.102.1 255.255.255.0
!
```

Figure 37:Config du Routage Inter-VLAN

#### 1.6.2.5 Configuration adresse IP Management de Switch d'accès

Nous avons créés l'adresse IP management du VLAN101 au niveau des switch layer 2.

Ci-dessous, un exemple de configuration dans le switch3 est illustré

```
!
interface Vlan101
  ip address 172.16.101.100 255.255.255.0
!
```

Figure 38:Config adresse IP Management

#### 1.6.2.6 Configuration de Serveur DHCP au niveau Router CE-Branch1

La figure suivante illustre la configuration du Serveur DHCP au niveau Router CE-Branch1 pour VLAN102, tel que les 10 premières adresses sont réservés

```
!
ip dhcp excluded-address 172.16.102.1 172.16.102.10
!
ip dhcp pool Data
  network 172.16.102.0 255.255.255.0
  default-router 172.16.102.1
  dns-server 8.8.8.8
!
```

Figure 39:Configuration de Serveur DHCP

### 1.7 Test et Validation des Services de la solution Re-dondante

#### 1.7.1 Test et validation du service DHCP au niveau des quatreVPCs

Les figures illustrent le fonctionnement du serveur DHCP au niveaux des quatres pcs.

```
PC1> ip dhcp
DORA IP 172.16.10.11/24 GW 172.16.10.1

PC1> [
```

Figure 40:ip dhcp pc1

```
PC2> ip dhcp
DDORA IP 172.16.15.11/24 GW 172.16.15.1

PC2> [
```

Figure 41:ip dhcp pc2

```

PC3> ip dhcp
DDORA IP 172.16.102.11/24 GW 172.16.102.1

PC3> █

```

Figure 42:ip dhcp pc3

```

PC4> ip dhcp
DDORA IP 172.16.104.11/24 GW 172.16.104.1

PC4> █

```

Figure 43:ip dhcp pc4

### 1.7.2 Test et validation du protocole de redondance HSRP

La figure suivante illustre le fonctionnement du protocole HSRP au niveau des deux switches fédérateurs

switches fédérateurs

```

federateur1#show standby brief
                  P indicates configured to preempt.
                  |
Interface  Grp  Pri  P State   Active           Standby          Virtual IP
Vl10       10    120  P Active  local            172.16.10.3      172.16.10.1
Vl15       15    120  P Active  local            172.16.15.3      172.16.15.1
Vl20       20    120  P Active  local            172.16.20.3      172.16.20.1
federateur1# █

```

Figure 44:test hsrp

```

federateur2#show standby brief
                  P indicates configured to preempt.
                  |
Interface  Grp  Pri  P State   Active           Standby          Virtual IP
Vl10       10    105  P Standby 172.16.10.2      local           172.16.10.1
Vl15       15    105  P Standby 172.16.15.2      local           172.16.15.1
Vl20       20    105  P Standby 172.16.20.2      local           172.16.20.1
federateur2# █

```

Figure 45:test hsrp

### 1.7.3 Test de Connexion entre les pc1,2,3,4

La figure suivante illustre le fonctionnement du routage inter VLAN

```

dhcp
DORA IP 172.16.10.11/24 GW 172.16.10.1

VPCS> ping 172.16.102.11

84 bytes from 172.16.102.11 icmp_seq=1 ttl=58 time=168.472 ms
84 bytes from 172.16.102.11 icmp_seq=2 ttl=58 time=213.498 ms
84 bytes from 172.16.102.11 icmp_seq=3 ttl=58 time=155.054 ms
84 bytes from 172.16.102.11 icmp_seq=4 ttl=58 time=156.744 ms
84 bytes from 172.16.102.11 icmp_seq=5 ttl=58 time=110.098 ms

VPCS> ping 172.16.15.11

84 bytes from 172.16.15.11 icmp_seq=1 ttl=63 time=45.969 ms
84 bytes from 172.16.15.11 icmp_seq=2 ttl=63 time=28.100 ms
84 bytes from 172.16.15.11 icmp_seq=3 ttl=63 time=26.434 ms
84 bytes from 172.16.15.11 icmp_seq=4 ttl=63 time=40.609 ms
84 bytes from 172.16.15.11 icmp_seq=5 ttl=63 time=27.165 ms

VPCS> ping 172.16.104.11

84 bytes from 172.16.104.11 icmp_seq=1 ttl=58 time=163.702 ms
84 bytes from 172.16.104.11 icmp_seq=2 ttl=58 time=182.214 ms
84 bytes from 172.16.104.11 icmp_seq=3 ttl=58 time=147.431 ms
84 bytes from 172.16.104.11 icmp_seq=4 ttl=58 time=201.361 ms
84 bytes from 172.16.104.11 icmp_seq=5 ttl=58 time=241.703 ms

VPCS> []

```

	sw3	CE12	CE22	sw4	fed1	CE11
dhcp						
DORA IP 172.16.15.11/24 GW 172.16.15.1						
VPCS> ping 172.16.104.11						
84 bytes from 172.16.104.11 icmp_seq=1 ttl=58 time=200.632 ms						
84 bytes from 172.16.104.11 icmp_seq=2 ttl=58 time=171.229 ms						
84 bytes from 172.16.104.11 icmp_seq=3 ttl=58 time=182.244 ms						
84 bytes from 172.16.104.11 icmp_seq=4 ttl=58 time=169.322 ms						
84 bytes from 172.16.104.11 icmp_seq=5 ttl=58 time=231.191 ms						
VPCS> ping 172.16.10.11						
84 bytes from 172.16.10.11 icmp_seq=1 ttl=63 time=45.876 ms						
84 bytes from 172.16.10.11 icmp_seq=2 ttl=63 time=32.015 ms						
84 bytes from 172.16.10.11 icmp_seq=3 ttl=63 time=19.558 ms						
84 bytes from 172.16.10.11 icmp_seq=4 ttl=63 time=33.603 ms						
84 bytes from 172.16.10.11 icmp_seq=5 ttl=63 time=28.600 ms						
VPCS> ping 172.16.102.11						
84 bytes from 172.16.102.11 icmp_seq=1 ttl=58 time=194.481 ms						
84 bytes from 172.16.102.11 icmp_seq=2 ttl=58 time=172.069 ms						
84 bytes from 172.16.102.11 icmp_seq=3 ttl=58 time=155.250 ms						
84 bytes from 172.16.102.11 icmp_seq=4 ttl=58 time=139.620 ms						
84 bytes from 172.16.102.11 icmp_seq=5 ttl=58 time=190.152 ms						
VPCS> []						

```

: | ● sw3 ● CE12 ● CE22 ● sw4 ● fed1

dhcp
DORA IP 172.16.102.11/24 GW 172.16.102.1

VPCS> ping 172.16.10.11

84 bytes from 172.16.10.11 icmp_seq=1 ttl=58 time=175.276 ms
84 bytes from 172.16.10.11 icmp_seq=2 ttl=58 time=234.319 ms
84 bytes from 172.16.10.11 icmp_seq=3 ttl=58 time=168.455 ms
84 bytes from 172.16.10.11 icmp_seq=4 ttl=58 time=157.037 ms
84 bytes from 172.16.10.11 icmp_seq=5 ttl=58 time=124.590 ms

VPCS> ping 172.16.15.11

84 bytes from 172.16.15.11 icmp_seq=1 ttl=58 time=179.072 ms
84 bytes from 172.16.15.11 icmp_seq=2 ttl=58 time=145.630 ms
84 bytes from 172.16.15.11 icmp_seq=3 ttl=58 time=168.311 ms
84 bytes from 172.16.15.11 icmp_seq=4 ttl=58 time=291.186 ms
84 bytes from 172.16.15.11 icmp_seq=5 ttl=58 time=139.893 ms

VPCS> ping 172.16.104.11

84 bytes from 172.16.104.11 icmp_seq=1 ttl=61 time=105.447 ms
84 bytes from 172.16.104.11 icmp_seq=2 ttl=61 time=75.014 ms
84 bytes from 172.16.104.11 icmp_seq=3 ttl=61 time=64.492 ms
84 bytes from 172.16.104.11 icmp_seq=4 ttl=61 time=78.011 ms
84 bytes from 172.16.104.11 icmp_seq=5 ttl=61 time=94.464 ms

VPCS> 

```

```

: | ● sw3 ● CE12 ● CE22 ● sw4 ● fed1 ● CE11

dhcp
DORA IP 172.16.104.11/24 GW 172.16.104.1

VPCS> ping 172.16.10.11

84 bytes from 172.16.10.11 icmp_seq=1 ttl=58 time=187.755 ms
84 bytes from 172.16.10.11 icmp_seq=2 ttl=58 time=169.778 ms
84 bytes from 172.16.10.11 icmp_seq=3 ttl=58 time=183.566 ms
84 bytes from 172.16.10.11 icmp_seq=4 ttl=58 time=185.342 ms
84 bytes from 172.16.10.11 icmp_seq=5 ttl=58 time=187.103 ms

VPCS> ping 172.16.15.11

84 bytes from 172.16.15.11 icmp_seq=1 ttl=58 time=189.975 ms
84 bytes from 172.16.15.11 icmp_seq=2 ttl=58 time=171.737 ms
84 bytes from 172.16.15.11 icmp_seq=3 ttl=58 time=369.775 ms
84 bytes from 172.16.15.11 icmp_seq=4 ttl=58 time=137.795 ms
84 bytes from 172.16.15.11 icmp_seq=5 ttl=58 time=170.259 ms

VPCS> ping 172.16.102.11

84 bytes from 172.16.102.11 icmp_seq=1 ttl=61 time=106.429 ms
84 bytes from 172.16.102.11 icmp_seq=2 ttl=61 time=63.717 ms
84 bytes from 172.16.102.11 icmp_seq=3 ttl=61 time=79.760 ms
84 bytes from 172.16.102.11 icmp_seq=4 ttl=61 time=67.229 ms
84 bytes from 172.16.102.11 icmp_seq=5 ttl=61 time=90.439 ms

VPCS> 

```

## 1.8 Conclusion

Dans ce chapitre, nous avons présenté l'architecture du réseau LAN étendu de Tekup.

Ensuite nous avons détaillé la conception de la Solution LAN puis nous avons exposé la

Description de la Solution Redondante de LAN. Ainsi nous avons passé au environnement

de travail Par la suite nous avons clarifiées la mise en place de la Solution de LAN

Redondante et nous avons fini par valider et tester la connexion pour assurer le bon

fonctionnement des services de la solution Redondante.

---

# CHAPITRE 3

---

## 1.1 Introduction

Dans ce chapitre, nous aborderons la conception et la mise en place de la solution

de monitoring et de sécurité AAA (Authentification, Autorisation et Accounting).

Nous

expliquerons les choix effectués pour la solution de monitoring et présenterons le modèle de

fonctionnement. Ensuite, nous détaillerons la mise en place de la solution, les tests réalisés

ainsi que la validation des résultats obtenus. Enfin, nous aborderons la description de la

solution AAA et sa mise en place, suivie des tests et de la validation des services de la

solution de sécurité AAA.

## 1.2 Choix de la Solution Monitoring

### 1.2.1 Etudes comparative des solutions de supervision

Avant de mettre en place la solution de monitoring, une étape cruciale consiste à choisir la meilleure solution adaptée à nos besoins. Le choix de cette solution de monitoring

dépend de plusieurs facteurs, tels que les besoins spécifiques de votre infrastructure, les

fonctionnalités requises, les contraintes techniques et budgétaires, ainsi que votre préférence personnelle. Voici quelques-unes des solutions populaires de monitoring :

1. Nagios : Nagios est considéré par certaines personnes comme le standard « de facto »

» dans le monitorage open source. Surtout, car il est le premier qui a bien fait.

Avant

Nagios, il y avait quelques options, mais ils étaient peu professionnels ou d'excellents

outils qui ne valaient que pour une tâche spécifique.

2. Zabbix : Zabbix est apparu un peu plus tard, en 2001. Il est complètement développé,

c'est pas un fourche de Nagios, et sa principale caractéristique est qu'il a une vision

plus holistique de la supervision, ce qui couvre pas seulement des états mais aussi la

performance, puisque c'est l'une des plus importantes carences de Nagios. En plus d'avoir

un système de gestion Web qui vous permet de le gérer de manière centralisée, sans la

complexité des fichiers de configuration, comme c'était le cas de Nagios.

3. Pandora FMS : Pandora FMS est né en 2004 et, comme Zabbix, est un développe-

ment qui part de zéro. Sa principale caractéristique c'est plus qu'un système de supervision

informatique il est un cadre de supervision qui permet de superviser l'infrastructure (ré-

seaux et serveurs), la performance, les applications et même la supervision des activités

métiers (APM).

### 1.2.2 Critères de choix des solutions de supervision

Nagios :

Nagios est un logiciel permettant de superviser le système et le réseau, qui s'appuie

sur 3 composants principaux :

- l'ordonnanceur, qui est le cœur de l'application et va se charger d'exécuter les sondes

de supervision à destination des éléments du SI ;

- l'interface Web, écrite en CGI et PHP, qui sert à visualiser les informations concernant les éléments supervisés ;

- les plugins, aussi appelées « sondes », qui ne sont finalement que de simples programmes lancés par l'ordonnanceur. Ces programmes fonctionnent de manière autonome

et fournissent simplement le résultat de la sonde à l'ordonnanceur.

Zabbix

Zabbix propose une solution de supervision technique et applicative, décomposée également en 3 composants :

- un serveur reposant sur un moteur de base de données tel que MySQL, PostgreSQL

ou Oracle ;

- une interface d'administration écrite en PHP permettant la visualisation des informations stockées en base, mais également la configuration des objets de supervision ;

- un nserveur de traitement, mettant à disposition plusieurs méthodes de supervision :

simples (comme celle d'un serveur Web par exemple), ou plus complexes (comme la charge

du processus ou l'espace disque. Le serveur requiert notamment l'installation d'un agent

sur la cible à superviser.

Cette solution se démarque en particulier par son interface. Zabbix est une solution

de supervision dite « full click » et s'adresse ainsi à un plus large public.

Centreon

Centreon a été créée à Toulouse par une entreprise nommée Merethis (renommée depuis

« Centreon », tout simplement). Ainsi, les premières versions de Centreon s'appuient sur

les concepts de Nagios et proposent une interface d'administration grâce à laquelle il

est possible, entre autres, de configurer les objets. Cette solution de supervision a les

caractéristiques suivantes :

- son architecture repose sur des technologies comme Apache et MySQL ;
- son architecture modulaire (Centreon Web, Centreon Broker, Centreon Engine)

lui permet de fonctionner sur des infrastructures réparties. Centreon propose son moteur

librement au téléchargement et des produits complémentaires (plugins, cartographie, etc.)

sous licence commerciale.

### 1.2.3 Solution proposé

L'adoption de Nagios par les entreprises du monde entier n'est pas fortuite.

Cette

plateforme apporte une série d'avantages significatifs qui améliorent la surveillance des

infrastructures IT, la gestion des performances et la prévention des pannes.

• Réduction des temps d'arrêt : En détectant les problèmes rapidement, Nagios aide

à minimiser les temps d'arrêt, ce qui peut économiser des ressources et réduire les coûts.

- Amélioration de la productivité : Permet aux équipes IT de se concentrer sur des

tâches à valeur ajoutée en automatisant la surveillance et la notification des problèmes.

- Flexibilité et personnalisation : Grâce à sa nature open source et à la disponibilité de

nombreux plugins, Nagios peut être adapté aux besoins spécifiques de chaque entreprise.

- Visibilité complète : Offre une vue d'ensemble et en détail de l'infrastructure IT, permettant une meilleure prise de décision et une réaction rapide aux incidents.

- Facilité de déploiement : Nagios est reconnu pour sa facilité d'installation et de configuration, permettant une mise en œuvre rapide de la surveillance.

- Communauté et support Bénéficie d'une large communauté d'utilisateurs et de développeurs, ainsi que de nombreuses ressources pour le support et le développement.

Nagios se révèle être une solution de surveillance IT extrêmement puissante et adapt-

table, idéale pour les administrateurs désireux de maintenir une infrastructure informative

tique performante et sécurisée. Grâce à son interface web conviviale, combinée à la puissance de la gestion en ligne de commande, et à une architecture extensible via une mul-

titude de plugins, Nagios offre une plateforme complète pour répondre à tous les besoins

de surveillance IT.

## 1.3 Model de fonctionnement de la Solution Moni-toring nagios

### 1.3.1 Fonctionnement

Nagios récupère les informations fournies par les services de surveillance et les analyse.

Si le résultat de cette analyse fait remonter un problème, les services de surveillance

peuvent envoyer des avertissements à l'administrateur du réseau de différentes manières :

courriers électroniques, messages instantanés, SMS, etc.

### 1.3.2 Architecture de nagios

Nagios peut être décomposé en trois parties :

- Un ordonnanceur, chargé de contrôler quand et dans quel ordre les contrôles des

services sont effectués.

- Une interface graphique qui affiche de manière claire et concise l'état des services

surveillés.

- Des greffons(ou sondes ou plugins), sont des petits scripts ou programmes qui sont

la base des vérifications.

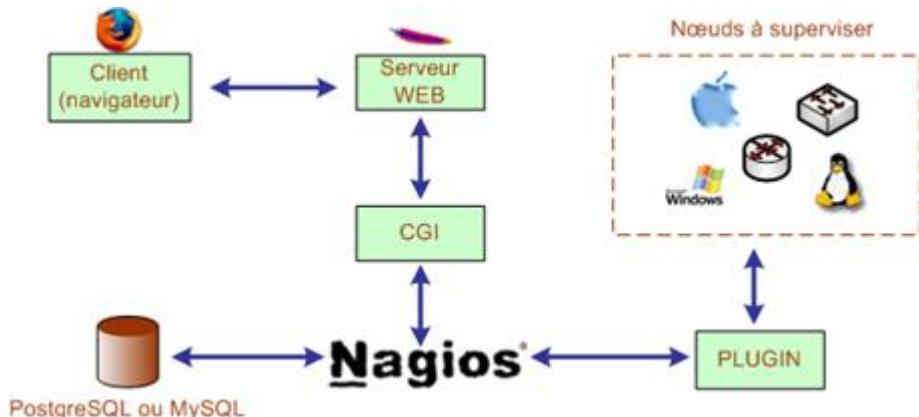


Figure 46:architecture standard de nagios

### 1.3.3 L'interface utilisée par Nagios

Dans notre cas, l'interface utilisée est le serveur web Apache. Apache est apparu en

avril 1995, fonctionne principalement sur les systèmes d'exploitation Unix et Windows.

Apache est conçu pour prendre en charge de nombreux modules lui donnant des fonctionnalités supplémentaires : interprétation du langage Perl, PHP, Python et Ruby, serveur

proxy, Common Gateway Interface, Server SideIncludes, réécriture d'URL, négociation de

contenu, protocoles de communication additionnels, etc.

#### 1.3.4 Le langage de programmation (ou serveur d'application)

PHP

PHP qui signifie Personal Home Page, est apparu en 1994, sous forme de petits outils

pour faciliter la vie des programmeurs web notamment grâce à Rasmus Lerdorf. PHP est

un langage de scripts. Il est interprété, par conséquent il ne nécessite pas d'être compilé

pour obtenir un objet, un exécutable avant d'être utilisable (comme en C par exemple).

PHP permet d'interfacer très facilement de très nombreuses bases de données notamment

MySQL gratuite et performante.

#### 1.3.5 Le serveur de bases de données MySQL

MySQL est un système de gestion de bases de données relationnelles (SGBDR). Il est

distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion

de base de données les plus utilisés au monde, autant par le grand public (applications

web principalement) que par des professionnels, en concurrence avec Oracle, Informix et

Microsoft SQL Server

### 1.3.6 . Le greffon

Nagios est un moteur d'ordonnancement de vérifications diverses assurées par des

greffons. La relation entre le moteur principal et les greffons se fait d'une part dans

la configuration de Nagios, pour que Nagios sache quelles vérifications lancer sur, ou à

destination, de quelles machines ou services ; d'autre part par le code retour ainsi que la

sortie standard d'un greffon.

Ces greffons (ou sondes ou plugins) fonctionnent soit en local sur la machine Nagios,

soit effectuent des tests à distance. Afin de pouvoir effectuer des vérifications plus poussées

sur une machine distante sans pour autant modifier la configuration de sécurité mise en

place, les créateurs de Nagios ont développé différents agents de transport et d'exécution de

test. Cette possibilité reprend une fonction définie par la norme ISO 7498/4 : la Structure

de gestion de réseaux (MNS)

Voici deux des principaux agents proposés par Nagios : • NRPE (Nagios Remote

Plugin Executor) : il constitue une méthode de surveillance dite active. En effet, l'initiateur

et l'ordonnanceur des tests est la machine nagios : le plugin check\_nrpe permet à la machine

Nagios d'envoyer des instructions aux daemon NRPE situé sur la machine distante.

• NSCA (Nagios Service Check Acceptor) : il s'agit là d'une méthode passive : le

client NSCA est installé, configuré et lancé sur chaque hôte distant de sorte à envoyer des

résultats de tests à la machine Nagios

### 1.3.7 Les principaux plugins

Les principaux plugins utilisés par NAGIOS sont :

- check-disk : Vérifie l'espace occupé d'un disque dur
- check-http : Vérifie le service "http" d'un hôte
- check-ftp : Vérifie le service "ftp" d'un hôte
- check-mysql : Vérifie l'état d'une base de données MYSQL
- check-nt : Vérifie différentes informations (disque dur, processeur ... )
- check-nrpe : Permet de récupérer différentes informations sur les hôtes
- check-ping : Vérifie la présence d'un équipement, ainsi que sa durée de réponse
- check-pop : Vérifie l'état d'un service POP (serveur mail)
- check-snmp : Récupère divers informations sur un équipement grâce au protocole

SNMP

## 1.4 Mise en place de la Solution Monitoring

### 1.4.1 L'architecture de la solution monitoring

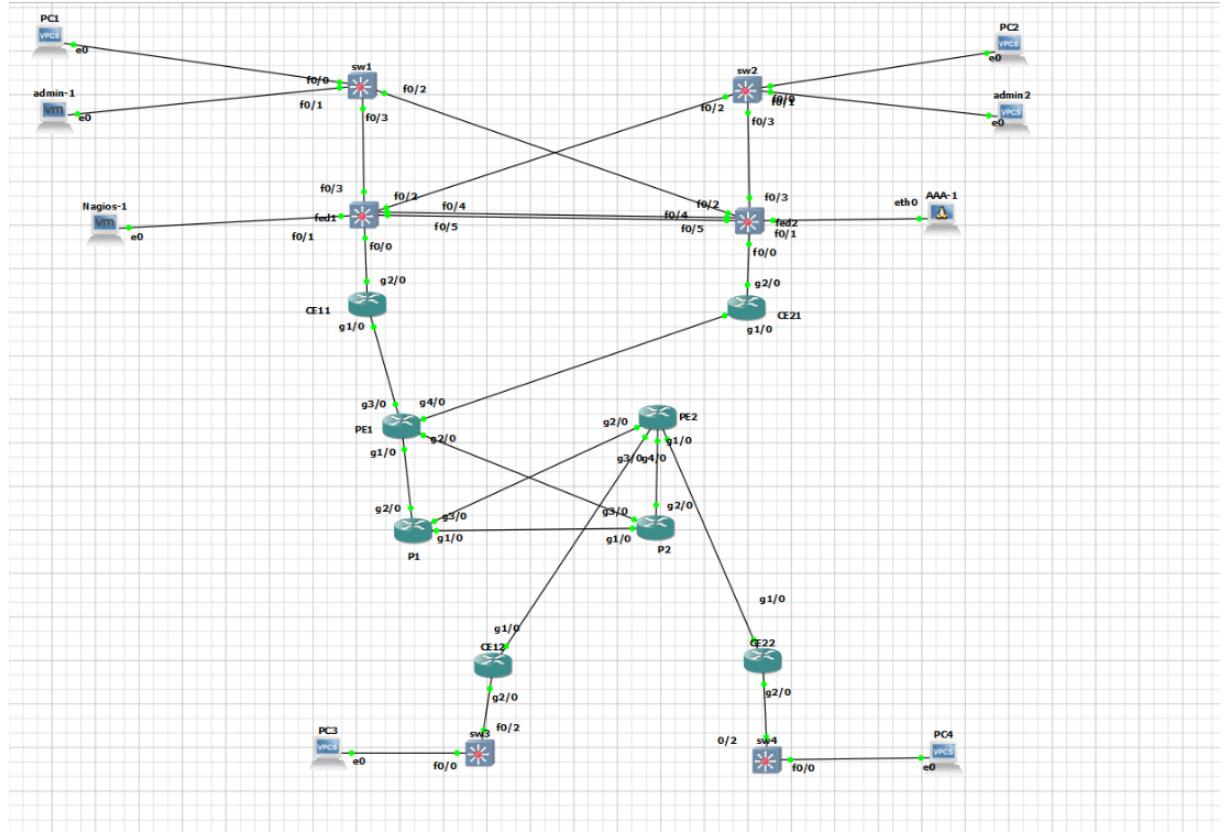


Figure 47:architecture sécurisée

### 1.4.2 Installer et configurer Nagios Core

1/ Mise à jour les packages système - sudo apt update

2/ Installation de tous les packages requis - sudo apt install wget unzip curl openssl

build-essential libgd-dev libssl-dev libapache2-mod-php php-gd php apache2 -y

3/ Télécharger les fichiers d'installation de Nagios Core - wget https://assets.nagios.com/downloads/

4.4.6.tar.gz

4/ Extraire les fichiers téléchargés. - sudo tar -zvxf nagios-4.4.6.tar.gz 5/ Accéder au

répertoire d'installation. - cd nagios-4.4.6

6/ Exécuter le script de configuration Nagios Core. - sudo ./configure

7/ Compiler le programme principal et les CGI. - sudo make all

8/ Créer et installer un groupe et un utilisateur. - sudo make install-groups-users

9/ Ajouter l'utilisateur des répertoires www-data au groupe nagios. - sudo usermod -a

-G nagios www-data

10/ Installer Nagios - sudo make install

11/Initialiser tous les scripts de configuration d'installation. - sudo make install-init

12/ Installer et configurer les autorisations sur le répertoire des configurations - sudo

make install-commandmode

13/Installer des exemples de fichiers de configuration - sudo make install-config

14/ Installer les fichiers Apache - sudo make install-webconf

15/Activer le mode de réécriture Apache - sudo a2enmod rewrite

16/ Activer la configuration CGI. - sudo a2enmod cgi

17/ Redémarrer le service Apache. - sudo systemctl restart apache2

18/ Créer un utilisateur et définir le mot de passe - sudo htpasswd -c /usr/local/nagios/etc/htpasswd

admin

#### 1.4.3 Installer les plugins Nagios

1/ Téléchargez le plugin Nagios Core - cd / - wget https://nagios-plugins.org/download/nagios-

plugins-2.3.3.tar.gz

2/ Extrayez le plugin téléchargé - sudo tar -zvxf nagios-plugins-2.3.3.tar.gz

3/ Accéder au répertoire des plugins - cd nagios-plugins-2.3.3/

4/ Exécutez le script de configuration du plugin - sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios

5/ Compiler les plugins Nagios Core - sudo make

6/ installer les plugins. - sudo make install

#### 1.4.4 Vérifier la configuration de Nagios

1/ Vérifier la configuration de Nagios Core - sudo /usr/local/nagios/bin/nagios -v  
/usr/local/nagios/etc/nagios.cfg

2/ Démarrer le service Nagios - sudo systemctl start nagios

3/ Activez le service Nagios pour qu'il s'exécute au démarrage du système - sudo  
sys-

temctl enable nagios

#### 1.4.5 Ajouter des hôtes distants

Pour surveiller les hôtes, nous devons les ajouter à Nagios. Par défaut, Nagios surveille

uniquement localhost (le serveur sur lequel il s'exécute).

Nous allons ajouter des hôtes qui font partie de notre réseau pour obtenir encore plus

de contrôle.

1/ installer nagios-plugins et nagios-nrpe-server : apt-get install nagios-plugins  
nagios-

nrpe-server

2/ Configure NRPE Ouvrir /etc/nagios/nrpe.cfg

```
GNU nano 6.2                               /etc/nagios/nrpe.cfg *
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1,::1,172.16.20.250

#
# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.
#
# *** ENABLING THIS OPTION IS A SECURITY RISK! ***
# Read the SECURITY file for information on some of the security implications
# of enabling this variable.
#
# Values: 0=do not allow arguments, 1=allow command arguments
#
dont_blame_nrpe=0

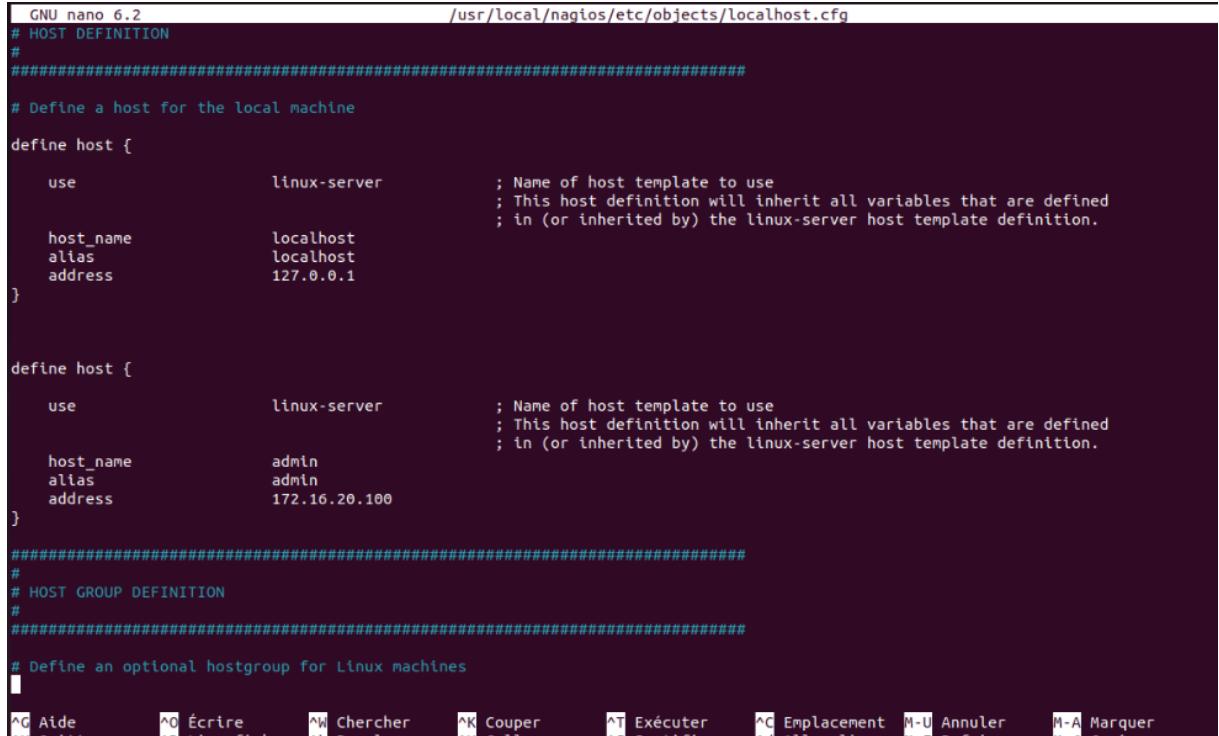
#
# BASH COMMAND SUBSTITUTION
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments that contain bash command substitutions of the form
# ${...}. This option only works if the daemon was configured with both
# the --enable-command-args and --enable-bash-command-substitution configure
# script options.
#
# *** ENABLING THIS OPTION IS A HIGH SECURITY RISK! ***
# Read the SECURITY file for information on some of the security implications
```

### 3/ Add the Host to Nagios

Maintenant que nous avons configuré l'hôte que nous allons surveiller, nous devons

revenir à notre serveur Nagios et y ajouter l'hôte

`nano /usr/local/nagios/etc/servers/host.cfg`



```
GNU nano 6.2                               /usr/local/nagios/etc/objects/localhost.cfg
#
#####
# Define a host for the local machine
#
define host {
    use            linux-server          ; Name of host template to use
                                         ; This host definition will inherit all variables that are defined
                                         ; in (or inherited by) the linux-server host template definition.
    host_name      localhost
    alias          localhost
    address        127.0.0.1
}

define host {
    use            linux-server          ; Name of host template to use
                                         ; This host definition will inherit all variables that are defined
                                         ; in (or inherited by) the linux-server host template definition.
    host_name      admin
    alias          admin
    address        172.16.20.100
}

#####
# HOST GROUP DEFINITION
#
#####

# Define an optional hostgroup for Linux machines
```

### 4/ Add the switches and the routers to Nagios

`nano /usr/local/nagios/etc/servers/switch.cfg`

```

GNU nano 6.2                               /usr/local/nagios/etc/objects/swtch.cfg
# HOST DEFINITIONS
#
#####
# Define the switch that we'll be monitoring

define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   sw1                 ; The name we're giving to this switch
    alias        sw1 Switch         ; A longer name associated with the switch
    address     172.16.20.101       ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}
define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   sw2                 ; The name we're giving to this switch
    alias        sw2 Switch         ; A longer name associated with the switch
    address     172.16.20.102       ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}
define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   sw3                 ; The name we're giving to this switch
    alias        sw3 Switch         ; A longer name associated with the switch
    address     172.16.101.100      ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}
define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   sw4                 ; The name we're giving to this switch
    alias        sw4 Switch         ; A longer name associated with the switch
    address     172.16.103.100      ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}

^G Aide          ^O Écrire        ^W Chercher      ^K Couper        ^T Exécuter      ^C Emplacement  M-U Annuler  M-A Marquer
^X Quitter      ^R Lire fich.  ^L Remplacer     ^U Coller        ^J Justifier    ^V Aller ligne  M-E Refaire  M-G Copier

```

```

GNU nano 6.2                               /usr/local/nagios/etc/objects/switch.cfg
address      172.16.103.100      ; IP address of the switch
hostgroups   switches           ; Host groups this switch is associated with
}
define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   fed1                ; The name we're giving to this switch
    alias        fed1 Switch        ; A longer name associated with the switch
    address     192.168.1.45        ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}
define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   fed2                ; The name we're giving to this switch
    alias        fed2 Switch        ; A longer name associated with the switch
    address     192.168.1.46        ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}
define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   CE11                ; The name we're giving to this switch
    alias        CE11 Router        ; A longer name associated with the switch
    address     172.16.11.11        ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}
define host {
    use          generic-switch      ; Inherit default values from a template
    host_name   CE12                ; The name we're giving to this switch
    alias        CE12 Router        ; A longer name associated with the switch
    address     172.16.12.12        ; IP address of the switch
    hostgroups  switches           ; Host groups this switch is associated with
}

^G Aide          ^O Écrire        ^W Chercher      ^K Couper        ^T Exécuter      ^C Emplacement  M-U Annuler  M-A Marquer
^X Quitter      ^R Lire fich.  ^L Remplacer     ^U Coller        ^J Justifier    ^V Aller ligne  M-E Refaire  M-G Copier

```

#### 4/ Rechargez Nagios service nagios reload

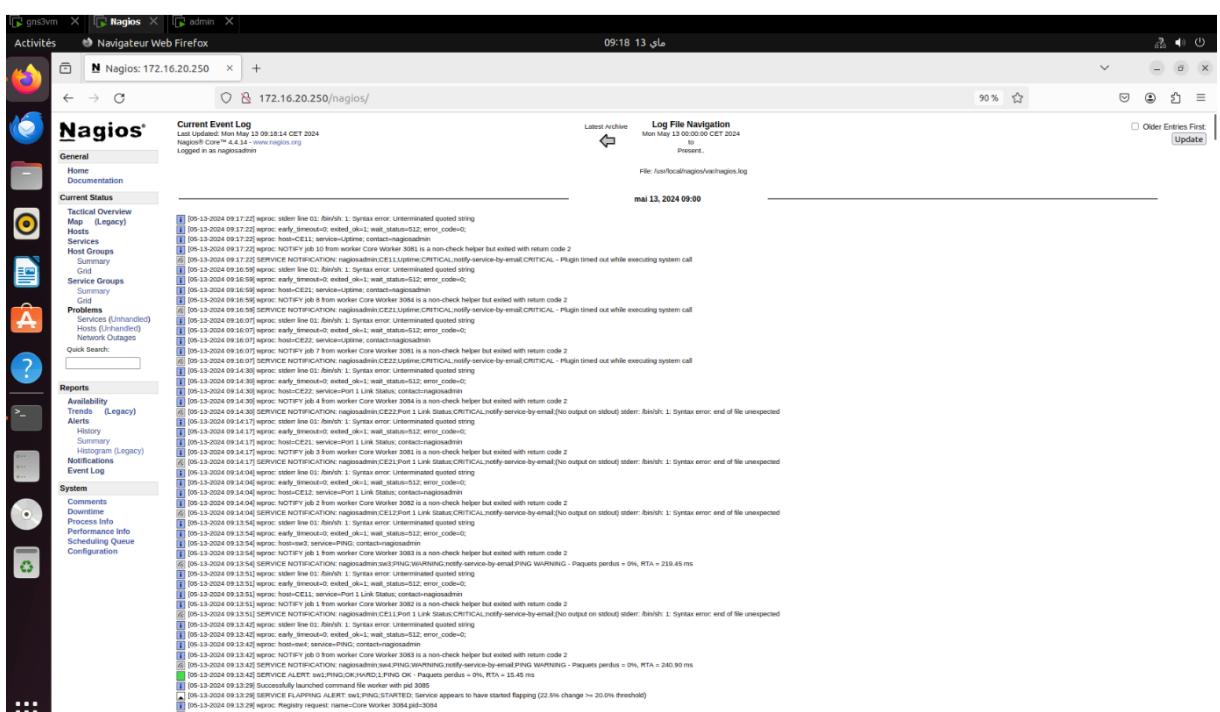
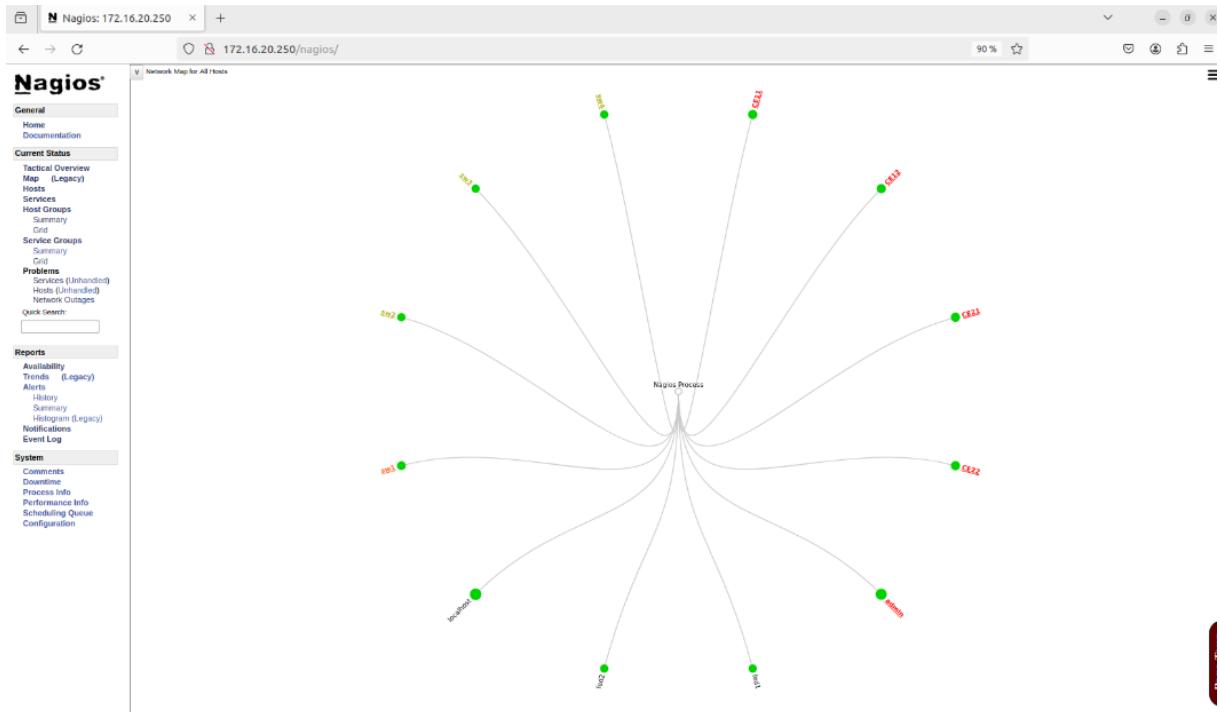
### 1.5 Test et Validation de la Solution Monitoring

The screenshot shows the Nagios web interface with the following sections:

- Current Network Status:** Last Updated: Monday, May 13 09:14:38 CET 2024. Nagios Core™ 4.4.14 - www.nagios.org.
- Host Status Totals:** Up: 12, Down: 0, Unreachable: 0, Pending: 0. All Problems: 0, All Types: 0.
- Service Status Totals:** OK: 12, Warning: 1, Unknown: 1, Critical: 1. All Problems: 1, All Types: 0.
- Host Status Details For All Host Groups:** Shows 12 hosts (CE01 to CE06, admin, and two others) with their last check times and duration.
- Service Status Details For All Host Groups:** Shows 24 services (Ping, Paquet perdus, RTA) with their last check times and duration.

The screenshot shows a Nagios web interface running on a Linux desktop environment. The main window displays the 'Host Status Totals' and 'Service Status Totals' for all hosts. A detailed table below lists each host's name, service, status, last check, duration, attempt, and status information. The table includes columns for host, service, status, last check, duration, attempt, and status information. The status information column contains detailed log entries for each host.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
CE11	PING	OK	05-13-2024 09:11:55	0d 0h 4m 0s	1/2	PING OK - Paquets perdus = 0%, RTA = 42.39 ms (No output on redbox stder: /bin/sh: 1: Syntax error: end of file unexpected)
CE11	Port 1 Link Status	CRITICAL	05-13-2024 09:13:51	0d 23h 57m 3s	3/3	CRITICAL - Plugin timed out while executing system call
CE11	Uptime	CRITICAL	05-13-2024 09:13:51	0d 23h 56m 14s	3/3	CRITICAL - Plugin timed out while executing system call
CE12	PING	OK	05-13-2024 09:11:28	0d 0h 4m 27s	1/2	PING OK - Paquets perdus = 0%, RTA = 1.00 ms
CE12	Port 1 Link Status	CRITICAL	05-13-2024 09:14:04	0d 23h 56m 48s	3/3	CRITICAL - No output on redbox stder: /bin/sh: 1: Syntax error: end of file unexpected
CE12	Uptime	CRITICAL	05-13-2024 09:14:00	0d 23h 56m 25s	3/3	CRITICAL - Plugin timed out while executing system call
CE21	PING	OK	05-13-2024 09:11:41	0d 0h 3m 34s	1/2	PING OK - Paquets perdus = 0%, RTA = 102.44 ms (No output on redbox stder: /bin/sh: 1: Syntax error: end of file unexpected)
CE21	Port 1 Link Status	CRITICAL	05-13-2024 09:13:17	0d 23h 56h 54s	3/3	CRITICAL - Plugin timed out while executing system call
CE21	Uptime	CRITICAL	05-13-2024 09:13:04	0d 23h 56m 47s	3/3	CRITICAL - Plugin timed out while executing system call
CE22	PING	OK	05-13-2024 09:11:45	0d 0h 3m 34s	1/2	PING OK - Paquets perdus = 0%, RTA = 161.31 ms (No output on redbox stder: /bin/sh: 1: Syntax error: end of file unexpected)
CE22	Port 1 Link Status	CRITICAL	05-13-2024 09:14:03	0d 23h 56m 48s	3/3	CRITICAL - No output on redbox stder: /bin/sh: 1: Syntax error: end of file unexpected
CE22	Uptime	CRITICAL	05-13-2024 09:13:05	0d 23h 56m 52s	3/3	CRITICAL - Plugin timed out while executing system call
admin	Current Users	OK	05-13-2024 09:12:07	0d 0h 4m 48s	1/2	UTILISATEURS OK - 2 utilisateurs actuellement connectés sur connect to address 172.25.20.100 and port 22: Connection refused
admin	HTTP	CRITICAL	05-13-2024 09:11:43	0d 7h 30m 15s	2/2	HTTP OK - Paquets perdus = 0%, RTA = 3.05 ms connect to address 172.25.20.100 and port 80: Connection refused
admin	PING	OK	05-13-2024 09:17:19	0d 0h 49m 48s	1/2	PING OK - Paquets perdus = 0%, RTA = 0.05 ms
admin	Root Partition	OK	05-13-2024 09:12:20	0d 7h 33m 52s	1/2	DISK OK - free space : 5413 MB (29% inobligatoires%) connect to address 172.25.20.100 and port 22: Connection refused
admin	SSH	CRITICAL	05-13-2024 09:11:56	0d 0h 37m 52s	1/2	SSH OK - 2 utilisateurs actuellement connectés sur connect to address 172.25.20.100 and port 22: Connection refused
admin	Swap Usage	OK	05-13-2024 09:07:32	0d 7h 47m 35s	1/2	SWAP OK - 100% libre (230 MB sur un total de 230 MB)
admin	Total Processes	OK	05-13-2024 09:12:33	0d 7h 45m 25s	1/2	PROCS OK - 133 processus avec ETTAT = PSSZT
root	PING	OK	05-13-2024 09:12:04	0d 0h 3m 11s	1/2	PING OK - Paquets perdus = 0%, RTA = 15.09 ms
root	Port 1 Bandwidth Usage	UNKNOWN	05-13-2024 09:12:27	0d 0h 3m 56s	1/2	PORT1 OK - 100% libre (70 MB sur un total de 70 MB)
root	SSH	OK	05-13-2024 09:12:46	0d 1h 4m 59s	1/2	SSH OK - charge moyenne : 0.00, 0.50, 0.50
root	Uptime	OK	05-13-2024 09:12:07	0d 1h 8m 21s	1/2	UTILISATEURS OK - 2 utilisateurs actuellement connectés sur
root	HTTP	OK	05-13-2024 09:12:11	0d 1h 7m 44s	1/2	HTTP OK - HTTP/1.1 200 OK - 3045 octets en 0.03 secondes de temps de réponse
root	PING	OK	05-13-2024 09:12:59	0d 1h 7m 6s	1/2	PING OK - Paquets perdus = 0%, RTA = 0.08 ms
root	Root Partition	OK	05-13-2024 09:12:40	0d 0h 47m 53s	1/2	DISK OK - free space : 5413 MB (29% inobligatoires%)
root	SSH	OK	05-13-2024 09:13:04	0d 1h 9m 51s	1/2	SSH OK - OpenSSH_8_5p1 LibreSSL-Subj-Berkeley-2.0 (protocol 2.0)
root	Swap Usage	OK	05-13-2024 09:13:12	0d 1h 9m 54s	1/2	SWAP OK - 100% libre (230 MB sur un total de 230 MB)
root	Total Processes	OK	05-13-2024 09:14:22	0d 0h 3m 36s	1/2	PROCS OK - 111 processus avec ETTAT = PSSZT
swx1	PING	OK	05-13-2024 09:13:38	0d 0h 3m 37s	1/2	PING OK - Paquets perdus = 0%, RTA = 15.45 ms
swx1	Port 1 Bandwidth Usage	UNKNOWN	05-13-2024 09:13:25	0d 1h 3m 29s	1/2	check_mrtg: impossible de ouvrir le fichier de log de MRTG
swx2	PING	WARNING	05-13-2024 09:14:57	0d 0h 10m 22s	3/3	PING WARNING - DUPLICATES FOUND Paquets perdus = 0%, RTA = 24.41 ms
swx2	PING	WARNING	05-13-2024 09:14:50	0d 0h 8m 26s	3/3	PING WARNING - Paquets perdus = 0%, RTA = 233.45 ms
swx2	Uptime	WARNING	05-13-2024 09:13:38	0d 0h 8m 37s	3/3	PING WARNING - Paquets perdus = 0%, RTA = 240.90 ms



Nagios®

**Current Network Status**

Last Updated: Mon May 13 09:21:49 CET 2024  
Updated every 99 seconds  
Nagios® Core™ 4.4.14 - www.nagios.org  
Logged in as nagiosadmin

**Host Status Totals**

Up	Down	Unreachable	Pending
12	0	0	0
All Problems	All Types		
0	12		

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
19	4	1	10	0
All Problems	All Types			
15	34			

**Host Status Details For All Host Groups**

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
CE11	UP	05-13-2024 09:18:56	0d 0h 12m 5s	PING OK - Paquets perdus = 0%, RTA = 40.20 ms
CE12	UP	05-13-2024 09:19:36	0d 0h 12m 1s	PING OK - Paquets perdus = 0%, RTA = 162.39 ms
CE21	UP	05-13-2024 09:19:20	0d 0h 12m 29s	PING OK - Paquets perdus = 0%, RTA = 101.85 ms
CE22	UP	05-13-2024 09:18:15	0d 0h 13m 34s	PING OK - Paquets perdus = 0%, RTA = 157.13 ms
admin	UP	05-13-2024 09:20:20	0d 1h 17m 29s	PING OK - Paquets perdus = 0%, RTA = 3.45 ms
fed1	UP	05-13-2024 09:18:16	0d 0h 13m 3s	PING OK - Paquets perdus = 0%, RTA = 18.95 ms
fed2	UP	05-13-2024 09:19:23	0d 0h 12m 26s	PING OK - Paquets perdus = 0%, RTA = 22.95 ms
localhost	UP	05-13-2024 09:21:35	1d 1h 15m 33s	PING OK - Paquets perdus = 0%, RTA = 0.08 ms
sw1	UP	05-13-2024 09:18:42	0d 8h 26m 23s	PING OK - Paquets perdus = 0%, RTA = 14.16 ms
sw2	UP	05-13-2024 09:17:49	1d 0h 30m 20s	PING WARNING - DUPLICATES FOUND! Paquets perdus = 0%, RTA = 19.50 ms
sw3	UP	05-13-2024 09:19:19	0d 0h 12m 30s	PING OK - Paquets perdus = 0%, RTA = 224.72 ms
sw4	UP	05-13-2024 09:18:16	0d 0h 12m 3s	PING OK - Paquets perdus = 0%, RTA = 228.03 ms

Results 1 - 12 of 12 Matching Hosts

Nagios®

**Current Network Status**

Last Updated: Mon May 13 09:22:21 CET 2024  
Updated every 99 seconds  
Nagios® Core™ 4.4.14 - www.nagios.org  
Logged in as nagiosadmin

**Host Status Totals**

Up	Down	Unreachable	Pending
12	0	0	0
All Problems	All Types		
0	12		

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
19	4	1	10	0
All Problems	All Types			
15	34			

**Service Status Details For All Hosts**

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
CE11	PING	OK	05-13-2024 09:21:15	0d 0h 1m 6s	1/3	PING OK - Paquets perdus = 0%, RTA = 35.88 ms (No output on stderr) stderr : /bin/sh: 1: Syntax error: end of file unexpected
	Port 1 Link Status	CRITICAL	05-13-2024 08:18:51	1d 0h 4m 9s	3/3	
	Uptime	CRITICAL	05-13-2024 08:18:27	1d 0h 0m 20s	3/3	CRITICAL - Plugin timed out while executing system call
CE12	PING	OK	05-13-2024 09:21:29	0d 0h 10m 52s	1/3	PING OK - Paquets perdus = 0%, RTA = 154.86 ms
	Port 1 Link Status	CRITICAL	05-13-2024 09:14:04	1d 0h 5m 55s	3/3	(No output on stderr) stderr : /bin/sh: 1: Syntax error: end of file unexpected
	Uptime	CRITICAL	05-13-2024 09:20:00	1d 0h 2m 7s	3/3	CRITICAL - Plugin timed out while executing system call
CE21	PING	OK	05-13-2024 09:21:41	0d 0h 10m 40s	1/3	PING OK - Paquets perdus = 0%, RTA = 98.22 ms
	Port 1 Link Status	CRITICAL	05-13-2024 09:14:17	1d 0h 0m 0s	3/3	(No output on stderr) stderr : /bin/sh: 1: Syntax error: end of file unexpected
	Uptime	CRITICAL	05-13-2024 09:16:04	1d 0h 3m 53s	3/3	CRITICAL - Plugin timed out while executing system call
CE22	PING	OK	05-13-2024 09:19:45	0d 0h 12m 36s	1/3	PING OK - Paquets perdus = 0%, RTA = 169.58 ms
	Port 1 Link Status	CRITICAL	05-13-2024 09:14:30	1d 0h 1m 47s	3/3	(No output on stderr) stderr : /bin/sh: 1: Syntax error: end of file unexpected
	Uptime	CRITICAL	05-13-2024 09:15:12	0d 23h 57m 58s	3/3	CRITICAL - Plugin timed out while executing system call
admin	Current Users	OK	05-13-2024 09:22:07	0d 0h 54m 52s	1/3	UTILISATEURS OK - 2 utilisateurs actuellement connectés sur
	HTTP	CRITICAL	05-13-2024 09:14:43	0d 7h 49m 24s	3/3	connect to address 172.16.20.100 and port 80: Connexion refusée
	PING	OK	05-13-2024 09:17:19	0d 7h 56m 52s	1/3	PING OK - Paquets perdus = 0%, RTA = 3.51 ms
	Root Partition	OK	05-13-2024 09:12:20	0d 7h 40m 58s	1/3	DISK OK - free space : 54213 MB (99% inode=60%)
	SSH	CRITICAL	05-13-2024 09:14:56	0d 7h 44m 34s	3/3	connect to address 172.16.20.100 and port 22: Connexion refusée
	Swap Usage	OK	05-13-2024 09:17:32	0d 7h 54m 41s	1/3	SWAP OK - 100% libre (2139 MB sur un total de 2139 MB)
	Total Processes	OK	05-13-2024 09:12:33	0d 7h 52m 35s	1/3	PROCS OK: 103 processus avec ETAT = RSDT
fed1	PING	OK	05-13-2024 09:22:04	0d 0h 10m 17s	1/3	PING OK - Paquets perdus = 0%, RTA = 10.78 ms
fed2	PING	OK	05-13-2024 09:17:37	0d 0h 9m 44s	1/3	PING OK - Paquets perdus = 0%, RTA = 29.37 ms
localhost	Current Load	OK	05-13-2024 09:17:46	1d 1h 16m 5s	1/4	OK - Charge moyenne: 0.72, 0.68, 0.60
	Current Users	OK	05-13-2024 09:18:07	1d 1h 15m 27s	1/4	UTILISATEURS OK - 2 utilisateurs actuellement connectés sur
	HTTP	CRITICAL	05-13-2024 09:22:11	1d 1h 14m 50s	1/4	HTTP OK - HTTP/1.1 200 - 1094 octets en 0.001 secondes de temps de réponse
	PING	OK	05-13-2024 09:17:59	1d 1h 14m 12s	1/4	PING OK - Paquets perdus = 0%, RTA = 0.07 ms
	Root Partition	OK	05-13-2024 09:21:40	0d 7h 54m 59s	1/4	DISK OK - free space : 54214 MB (99% inode=60%)
	SSH	CRITICAL	05-13-2024 09:19:30	1d 1h 12m 57s	1/4	SSH OK - OpenSSH_8.9p1 Ubuntu-Subuntu-0.7 (protocol 2.0)
	Swap Usage	OK	05-13-2024 09:18:12	1d 1h 12m 20s	1/4	SWAP OK - 100% libre (2139 MB sur un total de 2139 MB)
	Total Processes	OK	05-13-2024 09:19:22	1d 1h 11m 42s	1/4	PROCS OK: 111 processus avec ETAT = RSDT
sw1	PING	WARNING	05-13-2024 09:20:46	0d 0h 1m 35s	3/3	PING WARNING - DUPLICATES FOUND! Paquets perdus = 0%, RTA = 18.92 ms
	Port 1 Bandwidth Usage	UNKNOWN	05-13-2024 09:13:25	1d 1h 10m 34s	3/3	check_mrtg: Impossible d'ouvrir le fichier de log de MRTG

Page Tour

## 1.6 Description de la Solution AAA

L'authentification, l'autorisation et la comptabilité (AAA) est un cadre de sécurité qui

contrôle l'accès aux ressources informatiques, applique des politiques et audite l'utilisation.

L'AAA et ses processus combinés jouent un rôle majeur dans la gestion et la cybersécurité

du réseau en sélectionnant les utilisateurs et en assurant le suivi de leur activité pendant

qu'ils sont connectés.

### 1.6.1 les composants de solution AAA

Authentification

L'authentification implique qu'un utilisateur fournit des informations sur qui il est.

Les utilisateurs présentent des identifiants de connexion qui affirment qu'ils sont bien

ceux qu'ils prétendent. En tant qu'outil de gestion des identités et des accès (IAM),

un serveur AAA compare les informations d'identification d'un utilisateur à sa base de

données d'informations d'identification stockées en vérifiant si le nom d'utilisateur, le mot

de passe et d'autres outils d'authentification s'alignent sur cet utilisateur spécifique.

Les trois types d'authentification comprennent quelque chose que vous savez, comme

un mot de passe, quelque chose que vous avez, comme une clé USB (Universal Serial

Bus) et quelque chose que vous êtes, comme votre empreinte digitale ou d'autres données

biométriques.

## Autorisation

L'autorisation suit l'authentification. Pendant l'autorisation, un utilisateur peut se

voir accorder des priviléges pour accéder à certaines zones d'un réseau ou d'un système.

Les zones et les ensembles d'autorisations accordés à un utilisateur sont stockés dans

une base de données avec l'identité de l'utilisateur. Les priviléges de l'utilisateur peuvent

être modifiés par un administrateur. L'autorisation est différente de l'authentification

dans la mesure où l'authentification ne vérifie que l'identité d'un utilisateur, tandis que

l'autorisation dicte ce que l'utilisateur est autorisé à faire.

Par exemple, un membre de l'équipe informatique peut ne pas avoir les priviléges

nécessaires pour modifier les mots de passe d'accès pour un réseau privé virtuel (RPV)

à l'échelle de l'entreprise. Cependant, l'administrateur réseau peut choisir d'accorder des

priviléges d'accès aux membres, ce qui lui permet de modifier les mots de passe VPN des

utilisateurs individuels. De cette manière, le membre de l'équipe sera autorisé à accéder

à une zone dont il avait été précédemment interdit.

## Traçabilité

La comptabilité suit l'activité des utilisateurs pendant qu'ils sont connectés à un ré-

seau en suivant des informations telles que la durée de leur connexion, les données qu'ils

ont envoyées ou reçues, leur adresse IP (Internet Protocol), l'identifiant uniforme des

ressources (URI) qu'ils ont utilisé et les différents services auxquels ils ont accédé.

#### 1.6.2 l'importance du framework AAA dans la sécurité réseau

L'AAA est un élément crucial de la sécurité réseau, car elle limite les personnes ayant

accès à un système et assure le suivi de leur activité. De cette manière, les acteurs mal-

veillants peuvent être tenus à l'écart, et un acteur vraisemblablement bon qui abuse de ses

privileges peut faire l'objet d'un suivi de son activité, ce qui donne aux administrateurs

des informations précieuses sur leurs activités. Il existe deux principaux types d'AAA

pour la mise en réseau : l'accès au réseau et l'administration des appareils.

- Accès au réseau L'accès au réseau implique le blocage, l'octroi ou la limitation de

l'accès en fonction des informations d'identification d'un utilisateur. AAA vérifie l'identité

d'un appareil ou d'un utilisateur en comparant les informations présentées ou saisies à

une base de données d'identifiants approuvés. Si les informations correspondent, l'accès

au réseau est accordé.

- Administration des appareils L'administration des appareils implique le contrôle de

l'accès aux sessions, aux consoles des appareils réseau, à la couche de sécurité (SSH), etc.

Ce type d'accès est différent de l'accès au réseau, car il ne limite pas qui est autorisé à

accéder au réseau, mais plutôt les appareils auxquels il peut avoir accès.

### 1.6.3 Types de protocoles AAA

Il existe plusieurs protocoles qui intègrent les éléments de l'AAA pour assurer la sécurité de l'identité.

Service utilisateur d'authentification à distance (RADIUS)

RADIUS est un protocole réseau qui exécute des fonctions AAA pour les utilisateurs

sur un réseau distant à l'aide d'un modèle client/serveur. RADIUS fournit simultanément

l'authentification et l'autorisation aux utilisateurs qui tentent d'accéder au réseau. RA-

RADIUS prend également tous les paquets de données AAA et les chiffre, offrant un niveau

de sécurité supplémentaire.

RADIUS fonctionne en trois phases : l'utilisateur envoie une demande à un serveur

d'accès réseau (NAS), le NAS envoie ensuite une demande d'accès au serveur RADIUS,

qui répond à la demande en l'acceptant, en la rejetant ou en la remettant en question en

demandant plus d'informations.

Diamètre Le protocole Diameter est un protocole AAA qui fonctionne avec les réseaux

d'évolution à long terme (LTE) et multimédia. Le diamètre est une évolution de RADIUS,

qui a longtemps été utilisé pour les télécommunications. Cependant, Diameter est conçu

sur mesure pour optimiser les connexions LTE et d'autres types de réseaux mobiles.

Contrôleur d'accès aux terminaux - Système de contrôle d'accès Plus (TACACS+) Tout comme RADIUS, TACACS+ utilise le modèle client/serveur pour connecter les utilisateurs. Cependant, TACACS+ permet de mieux contrôler les manières dont les

commandes sont autorisées. TACACS+ fonctionne en fournissant une clé secrète connue

du client et du système TACACS+. Lorsqu'une clé valide est présentée, la connexion est

autorisée à continuer.

TACACS+ sépare les processus d'authentification et d'autorisation, ce qui le différencie de RADIUS, qui les combine. De plus, TACACS+, comme RADIUS, chiffre ses

paquets AAA.

## 1.7 Mise en place de la Solution de sécurité AAA de

Tekup

### 1) configuration de AAA

```
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
```

```
!
radius-server host 172.16.20.200
radius-server key VPN_SSIR
!
```

```
!
ip access-list extended T0-CE11
 permit tcp host 172.16.20.100 host 172.16.11.11 range 22 telnet
 permit tcp host 172.16.20.150 host 172.16.11.11 range 22 telnet
 deny ip any any log
!
```

## 1.8 Test et Validation des Services de la solution de sécurité AAA

### 1.9 conclusion

Dans ce chapitre, nous avons exploré la mise en place de la solution AAA pour le monitoring et la sécurité. Nous avons d'abord décrit les choix stratégiques pour le système

de monitoring, son modèle de fonctionnement, puis détaillé sa mise en œuvre, les tests réalisés et les résultats obtenus. Ensuite, nous avons présenté la solution AAA, expliqué son déploiement et les tests de validation pour garantir son bon fonctionnement. En bref,

ce chapitre couvre la conception, l'implémentation et la validation de la solution AAA, soulignant son rôle crucial dans la surveillance et la sécurisation des systèmes et réseaux.