

srv-logs

MARK RODERICK - supervision et journalisation- logs

[3.5.4 Prévention des attaques](#) [3.5.5 Détection des actions malveillantes](#)

[3.5.6 Analyse d'incidents de sécurité, proposition et mise en œuvre de contre-mesures](#)

1. C'est quoi un "Log" ? (Le Journal de Bord)

Un **log** (ou "journalisation" en français) est un enregistrement chronologique de tout ce qui se passe sur un système, une application ou un équipement réseau. C'est comme la boîte noire d'un avion ou un journal intime numérique.

Chaque ligne de log contient généralement :

- **L'horodatage (Timestamp)** : Quand ça s'est passé.
 - **La source** : Quelle machine ou application a généré l'événement.
 - **Le niveau de gravité** : (INFO, WARNING, ERROR, CRITICAL).
 - **Le message** : La description de ce qui s'est passé (ex: "Échec de connexion pour l'utilisateur admin").
-

2. Pourquoi les logs sont-ils importants ?

Sans logs, tu es aveugle. Voici les quatre raisons majeures de leur importance :

1. **Dépannage (Troubleshooting)** : Quand un serveur plante à 3h du matin, le log te dit précisément quelle erreur a causé l'arrêt.
 2. **Sécurité** : Si quelqu'un tente de forcer un mot de passe (Brute Force), les logs de sécurité enregistrent toutes les tentatives infructueuses. C'est la base pour détecter une intrusion.
 3. **Analyse de performance** : Les logs permettent de voir si une application devient lente ou si un disque dur commence à montrer des signes de faiblesse.
 4. **Conformité légale** : Dans beaucoup de pays et d'industries (banque, santé), la loi oblige à conserver les logs pendant une certaine durée (souvent 1 an) pour pouvoir enquêter en cas d'incident.
-

3. C'est quoi un Serveur de Logs ? (La Centralisation)

Dans un petit réseau, tu peux aller lire les logs directement sur chaque machine. Mais si tu as 50 serveurs, 10 switches et 5 pare-feu, c'est impossible. C'est là qu'intervient le **Serveur de Logs centralisé**.

Le principe :

Toutes tes machines envoient leurs logs en temps réel vers un serveur unique (souvent via un protocole appelé **Syslog**).

4. Pourquoi centraliser les logs sur un serveur dédié ?

Avoir un serveur de logs spécifique présente des avantages stratégiques :

Avantage	Pourquoi c'est crucial ?
Persistance	Si un pirate efface les logs sur le serveur qu'il a hacké pour cacher ses traces, les logs sont déjà sauvegardés en sécurité sur ton serveur de logs central.
Corrélation	Tu peux voir que l'erreur sur la base de données (Serveur A) est liée à une tentative de connexion suspecte sur le Pare-feu (Machine B).
Vitesse de recherche	Au lieu de te connecter à 10 machines, tu fais une seule recherche globale (ex: "Chercher 'Erreur 500' partout").
Alerte	Le serveur de logs peut t'envoyer un mail ou un SMS dès qu'il voit passer le mot "CRITICAL" dans un flux.

Les outils populaires (Le "Stack")

Si tu veux monter un serveur de logs, tu entendras souvent parler de ces solutions :

- **ELK Stack** : Le trio le plus célèbre (Elasticsearch pour stocker, Logstash pour trier, Kibana pour visualiser sous forme de jolis graphiques).
- **Graylog** : Très puissant et souvent plus simple à gérer que ELK.
- **Splunk** : La Rolls-Royce (très puissant, mais payant et cher).
- **RSyslog / Syslog-ng** : Les outils de base sous Linux pour transférer les logs d'une machine à l'autre.

En résumé : Le log est la **preuve** de ce qui s'est passé. Le serveur de logs est le **coffre-fort** et la **loupe** qui te permet d'analyser ces preuves rapidement.

Est-ce que tu veux que je t'explique comment on configure une machine pour qu'elle envoie ses logs vers un serveur (le protocole Syslog) ?

Objectif :

Mise en place d'une VM utilisant Debian 13 On utilisera la solution LogAnalyser Contexte TP
Mettre en place et récupération de logs.

Objectif :

Centraliser les logs sur LogAnalyser (copier les logs de : --> logs de cisco, des stormshield, des AD DNS) Réalisation TP On va mettre en place une Debian 13 en utilisant une image ISO, elle sera de gen1

Définition d'un SIEM

Un **SIEM (Security Information and Event Management)** est une solution de cybersécurité qui permet de **collecter, centraliser et analyser les journaux (logs)** provenant des systèmes, applications et équipements réseau. Ses objectifs principaux sont :

- **Détection des menaces** en temps réel grâce à la corrélation des événements.
- **Surveillance de la sécurité** et visibilité complète sur l'infrastructure.
- **Conformité réglementaire** (ex. RGPD, ISO 27001, PCI-DSS) via des rapports et audits.
- **Réponse aux incidents** plus rapide grâce aux alertes et automatisations.

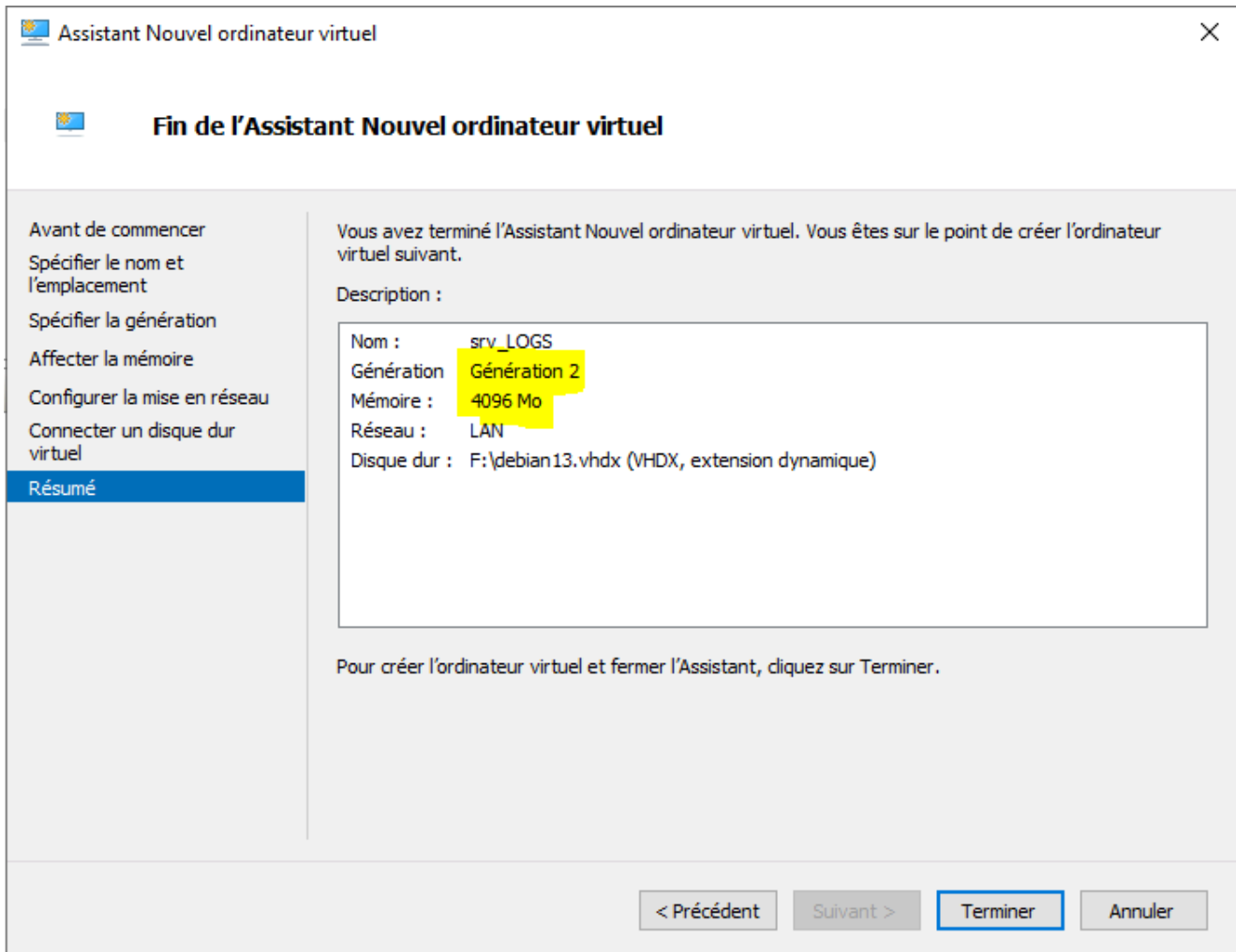
Comparatif des principaux SIEM

Outil	Type / Modèle	Points forts	Cas d'usage idéal
Splunk Enterprise Security	Logiciel propriétaire, niveau entreprise	Analyses en temps réel, tableaux de bord personnalisables, nombreuses intégrations	Grandes entreprises nécessitant une visibilité complète et conformité
ELK Stack (Elastic SIEM)	Open source	Flexible, évolutif, économique, recherche puissante	Équipes techniques, startups, PME avec contraintes budgétaires
Graylog Security	Open source	Facile à utiliser, personnalisable, abordable, bonne gestion des logs	PME ou organisations cherchant un SIEM léger
IBM QRadar	Logiciel propriétaire, niveau entreprise	Détection avancée des menaces, rapports de conformité, moteur de corrélation puissant	Secteurs réglementés (finance, santé, administrations)
Exabeam Fusion SIEM	Logiciel propriétaire, nouvelle génération	Analyse du comportement des utilisateurs (UEBA), automatisation, machine learning	Entreprises axées sur la détection des menaces internes et l'automatisation

- **Splunk & IBM QRadar** → puissants, adaptés aux grandes organisations et aux environnements réglementés.

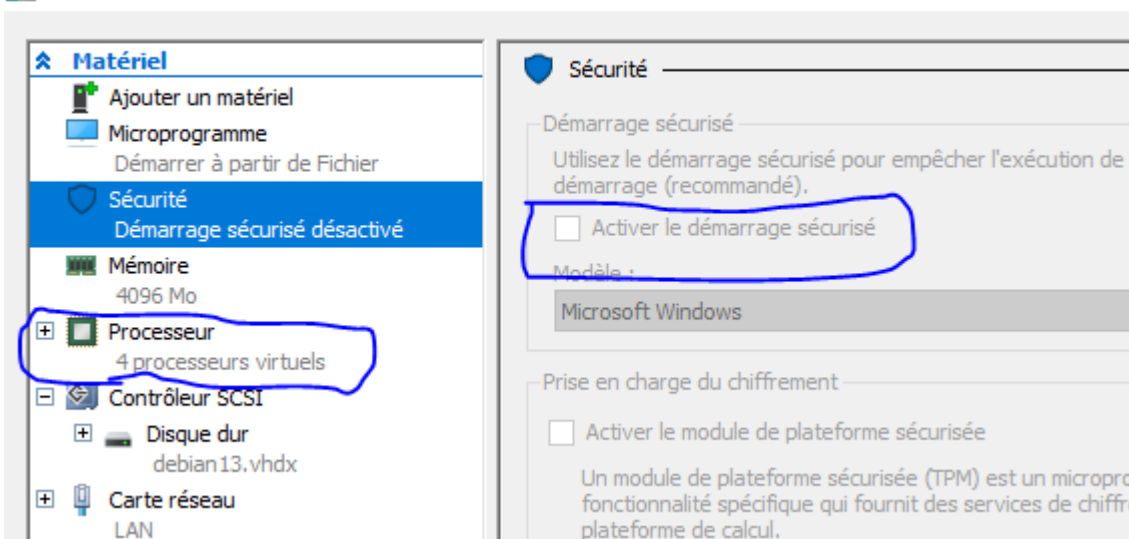
- **ELK & Graylog** → flexibles, open source, économiques, parfaits pour PME et équipes techniques.
- **Exabeam** → moderne, centré sur l'automatisation et l'analyse comportementale.

Debian 13 srv de logs

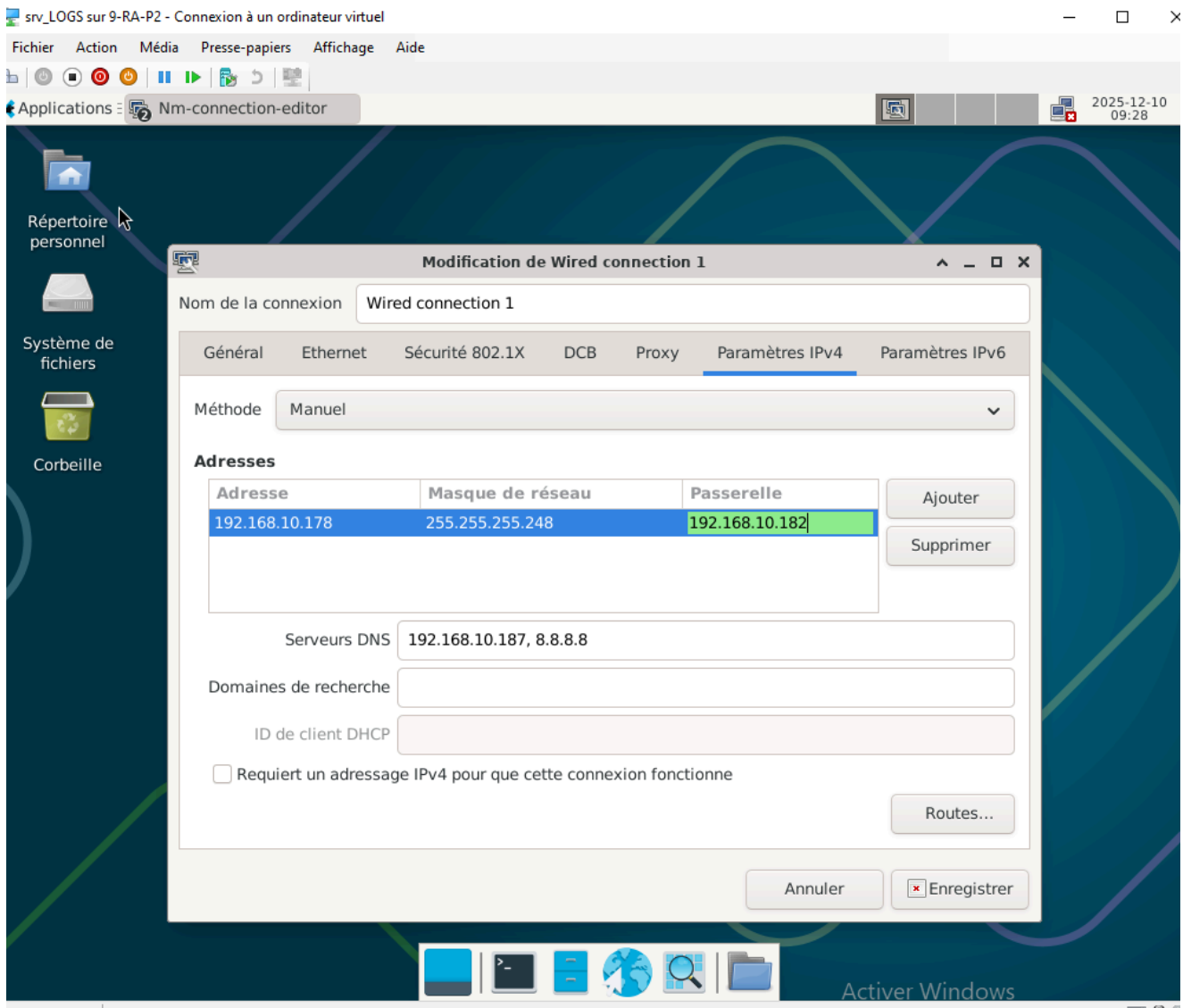


POUR FACILITER LA DEMARRAGE DU VM

Paramètres pour srv_LOGS sur 9-RA-P2



connexion reseau



passerelle

```

Administrateur: Invite de commandes
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

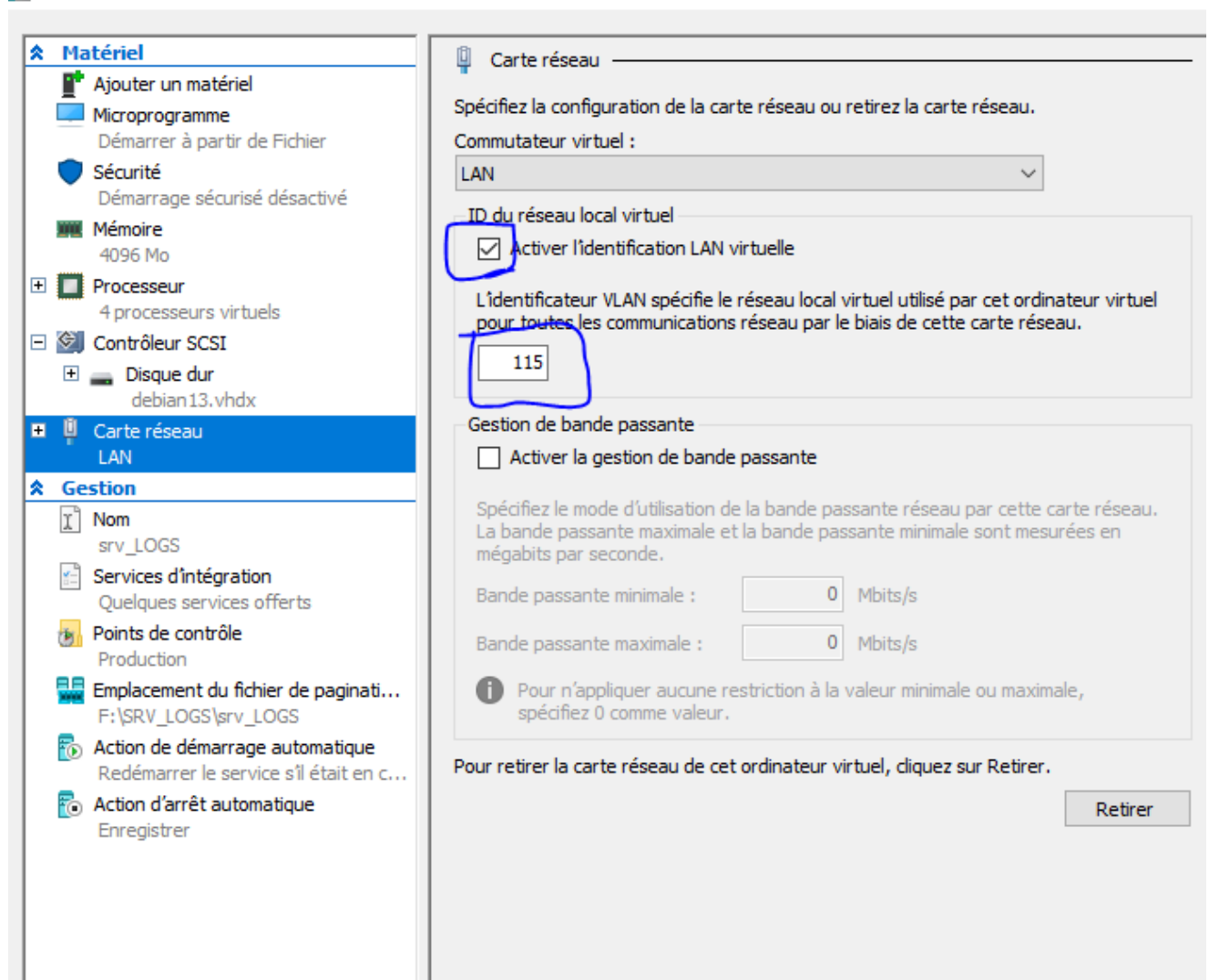
    Nom de l'hôte . . . . . : srvsptb
    Suffixe DNS principal . . . . . : STPetesbourg.lan
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: STPetesbourg.lan

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Description. . . . . : Microsoft Hyper-V Network Adapter
    Adresse physique . . . . . : 00-15-5D-03-36-8A
    DHCP activé. . . . . : Non
    Configuration automatique activée. . . : Oui
    Adresse IPv4. . . . . : 192.168.10.187(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.248
    Passerelle par défaut. . . . . : 192.168.10.190
    Serveurs DNS. . . . . : 192.168.10.187
    . . . . . : 8.8.8.8
    NetBIOS sur Tcpip. . . . . : Activé

C:\Users\Administrateur>
  
```

srv de logs dans le vlan it = 115



Installation apache 2

A. Installer Apache sous Debian 13

Nous commençons par mettre à jour le cache des paquets :

```
sudo apt update
```

Ensuite, nous installons le paquet **apache2** afin d'obtenir la dernière version d'Apache 2.4.

```
sudo apt install -y apache2
```

Pour qu'Apache démarre automatiquement au démarrage de la machine, saisissez la commande ci-dessous (même si normalement c'est déjà le cas) :

```
sudo systemctl enable apache2
```

```
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install
```

```
Executing: /lib/systemd/systemd-sysv-install enable apache2
```

Suite à l'installation du paquet, le serveur Apache démarre directement. D'ailleurs, nous devrions pouvoir accéder à la page par défaut du serveur Web Apache2. Pour cela, il suffit de récupérer l'adresse IP du serveur :

```
ip address
```

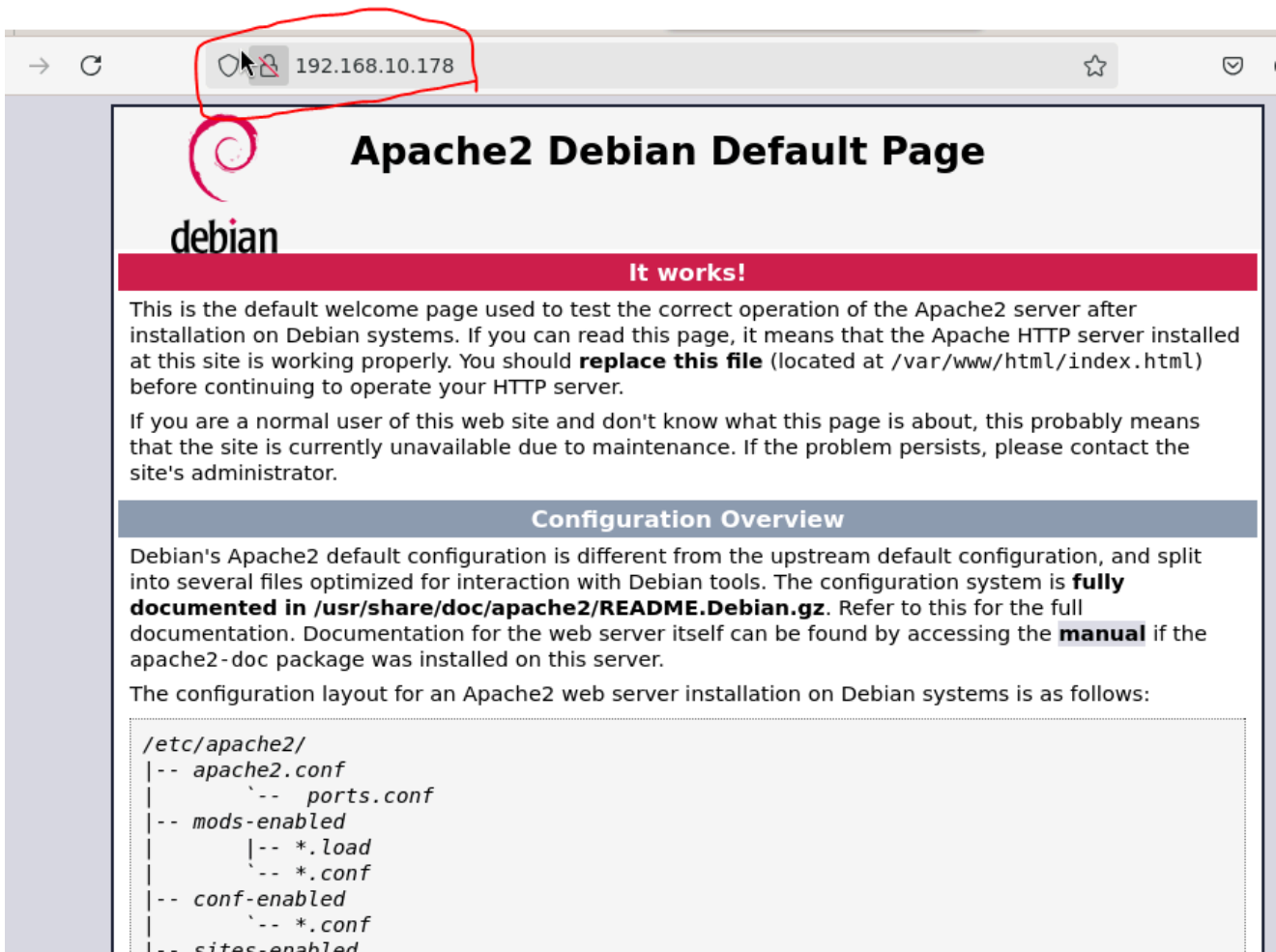
Puis, à l'aide d'une machine équipée d'un navigateur, nous pouvons accéder à notre serveur Apache

ip du debian 13

```
root@debian13:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN g
t qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
ult qlen 1000
  link/ether 00:15:5d:03:36:91 brd ff:ff:ff:ff:ff:ff
  atname enx00155d033691
  inet 192.168.10.178/29 brd 192.168.10.183 scope global noprefixro
    valid_lft forever preferred_lft forever
  inet6 fe80::23de:9566:5ff1:285c/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
root@debian13:~#
```

sur une navigateur web

<http://192.168.10.178> pour aller sur l'interface graph du debian



pour visualiser apache qu'on viens d'installer
avec la commande `sudo apache2ctl -v`

```
root@debian13:~# sudo apache2ctl -v
Server version: Apache/2.4.65 (Debian)
Server built:   2025-07-29T17:52:31
root@debian13:~#
```

activate new config

```
root@debian13:~# sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
systemctl restart apache2
root@debian13:~#
```

Activons quatre autres modules :

- **deflate** pour la gestion de la compression, notamment en gzip, pour utiliser la mise en cache des pages sur votre site
- **headers** afin de pouvoir agir sur les en-têtes HTTP
- **ssl** pour gérer les certificats SSL et donc l'utilisation du protocole HTTPS
- **http2** pour gérer les connexions HTTP/2

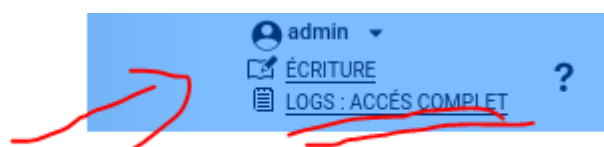
```
sudo a2enmod deflate headers ssl http2
```

```
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure S
elf-signed certificates.
Enabling module http2.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@debian13:~# sudo a2enmod rewrite
Module rewrite already enabled
root@debian13:~# sudo a2enmod deflate headers ssl http2
Considering dependency filter for deflate:
Module filter already enabled
Module deflate already enabled
Module headers already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
Module http2 already enabled
root@debian13:~#
```

POUR jointe le stormshield interne aux serveur de logs

ip srv de logs = 192.168.10.178

sts_interne=172.16.10.250



MONITORING CONFIGURATION EVA1 sts-interne

admin ÉCRITURE LOGS : ACCES RESTREINT

NOTIFICATIONS / TRACES - SYSLOG - IPFIX

STOCKAGE LOCAL **SYSLOG** IPFIX

PROFILS SYSLOG

État	Nom
Activé	Syslog Profile 0
Désactivé	Syslog Profile 1
Désactivé	Syslog Profile 2
Désactivé	Syslog Profile 3

Détails

Nom: Syslog Profile 0

Commentaire:

Serveur Syslog: **srv_logs**

Protocole: UDP

Port: **syslog**

Autorité de certification:

Certificat serveur:

Certificat client:

Format: RFC5424

Configuration avancée

ANNULER APPLIQUER

sur le srv de logs apres la commutation

LogAnalyzer ANALYSIS & REPORTING

Select Language: English

Select a Style: Default

Select Source: Srv-log

Select View: Syslog Fields

Search (filter):

Recent syslog messages

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 13:21:21	USER	NOTICE	sts-interne	serverd	UNKNOWN	Syslog	time="2025-12-10 13:21:21" fw="sts-interne" tz=+0100 starttime="20 ...
Today 13:21:21	USER	NOTICE	sts-interne	routerd	UNKNOWN	Syslog	time="2025-12-10 13:21:21" fw="sts-interne" tz=+0100 starttime="20 ...
Today 13:21:21	USER	NOTICE	sts-interne	routerd	UNKNOWN	Syslog	time="2025-12-10 13:21:21" fw="sts-interne" tz=+0100 starttime="20 ...
Today 13:21:21	USER	ERR	sts-interne	asqd	UNKNOWN	Syslog	time="2025-12-10 13:21:21" fw="sts-interne" tz=+0100 starttime="20 ...
Today 13:21:21	USER	WARNING	sts-interne	asqd	UNKNOWN	Syslog	time="2025-12-10 13:21:21" fw="sts-interne" tz=+0100 starttime="20 ...
Today 13:21:21	USER	NOTICE	sts-interne	serverd	UNKNOWN	Syslog	time="2025-12-10 13:21:21" fw="sts-interne" tz=+0100 starttime="20 ...
Today 13:21:20	USER	NOTICE	sts-interne	routerd	UNKNOWN	Syslog	time="2025-12-10 13:21:20" fw="sts-interne" tz=+0100 starttime="20 ...

switch cisco

Pour connecter son cisco au srv_logs

- Faut laisser une carte reseau sans vlan
-

Small Business
SG300-10 10-Port Gigabit Managed Switch

Remote Log Servers

IPv4 Source Interface: Auto
IPv6 Source Interface: Auto

Apply Cancel

Remote Log Server Table

<input type="checkbox"/>	Log Server	UDP Port	Facility	Description	Minimum Severity
<input type="checkbox"/>	192.168.12.178	514	Local 6	direction SRV Log	Informational
<input type="checkbox"/>	192.168.10.178	514	Local 7	srv_logs	Informational

Add... Edit... Delete

Small Business
SG300-10 10-Port Gigabit Managed Switch

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to 113
AND Interface Type equals to Port Go

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Trunk	Excluded	<input type="checkbox"/>
GE2	Trunk	Excluded	<input type="checkbox"/>
GE3	Trunk	Tagged	<input type="checkbox"/>
GE4	Trunk	Excluded	<input type="checkbox"/>
GE5	Trunk	Excluded	<input type="checkbox"/>
GE6	Trunk	Excluded	<input type="checkbox"/>
GE7	Trunk	Excluded	<input type="checkbox"/>
GE8	Trunk	Excluded	<input type="checkbox"/>
GE9	Trunk	Excluded	<input type="checkbox"/>
GE10	Trunk	Excluded	<input type="checkbox"/>

Apply Cancel

puis sur le sts interne
on desactive la ligne wifi

Rechercher...

+ Nouvelle règle X Supprimer

	État	Action	Source	Destination	Port dest.	Protocole	Inspection
Default policy 1 à 8 (contient 12 règles, de 4 à 15)							
4	on	passer	Network_client1 interface: client1	Internet	http https		IPS
5	on	passer	Network_client2	Internet	http https		IPS
6	on	passer	Network_srv_prod interface: srv_prod	Internet	*	Any	IPS
7	on	passer	Network_srv_auth interface: srv_auth	Internet	*	Any	IPS
8	off	passer	Network_wifi	Internet	http https		IPS
9	on	passer	Network_in interface: in	Internet	*	Any	IPS
10	off	bloquer	Any	Any	Any		IPS

dans reseau sur sur sts interne
on change ladress ip au 192.168.11.253/24

RESEAU / INTERFACES

Entrez un filtre...

DMZ
in
client1
client2
wifi
srv_prod
srv_it
srv_auth

CONFIGURATION DE WIFI

CONFIGURATION GÉNÉRALE CONFIGURATION AVANCÉE

Cette interface est: Interne (protégée)

Plan d'adressage

Adressage: Plan d'adressage hérité du bridge
 IP dynamique (obtenue par DHCP)

Adresse IPv4: IP dynamique (obtenue par DHCP)

Adresse / Masque	Commentaire
192.168.11.253/24	

VÉRIFICATION DE LA CONFIGURATION

encoere sur le cisco

ipv4 interface

Non sécurisé 192.168.5.254/cs950543f4/home.htm

Small Business
CISCO SG300-10 10-Port Gigabit Managed Switch

Getting Started
 Status and Statistics
 Administration
 Port Management
 Smartport
 VLAN Management
 Spanning Tree
 MAC Address Tables
 Multicast
IP Configuration
 IPv4 Management and Interface
 IPv4 Interface
 IPv4 Routes
 ARP
 ARP Proxy
 UDP Relay/IP Helper
 DHCP Snooping/Relay
 DHCP Server
 IPv6 Management and Interface
 Domain Name System
 Security
 Access Control
 Quality of Service
 SNMP

IPv4 Interface

Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/> VLAN 1	Static	192.168.5.254	255.255.255.0	Valid
<input type="checkbox"/> VLAN 123	Static	192.168.13.254	255.255.255.0	Valid

Add... Edit... Delete

Add IP Interface - Profil 1 - Microsoft Edge

Non sécurisé 192.168.5.254/cs950543f4/ipaddr/system_ipconf_ipInterface_...

Interface: Port GE1 LAG 1 VLAN 113 Loopback

IP Address Type: Dynamic IP Address Static IP Address

IP Address: 192.168.11.254

Mask: Network Mask Prefix Length 24 (Range: 8 - 30)

Apply Close

resultat

Small Business
CISCO SG300-10 10-Port Gigabit Managed Switch

Getting Started
 Status and Statistics
 Administration
 Port Management
 Smartport
 VLAN Management
 Spanning Tree
 MAC Address Tables
 Multicast
IP Configuration
 IPv4 Management and Interface
 IPv4 Interface
 IPv4 Routes
 ARP
 ARP Proxy

IPv4 Interface

Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/> VLAN 1	Static	192.168.5.254	255.255.255.0	Valid
<input type="checkbox"/> VLAN 113	Static	192.168.11.254	255.255.255.0	Valid
<input type="checkbox"/> VLAN 123	Static	192.168.13.254	255.255.255.0	Valid

Add... Edit... Delete

ipv4 routes

Small Business
SG300-10 10-Port Gigabit Managed Switch

Getting Started
 ▶ Status and Statistics
 ▶ Administration
 ▶ Port Management
 ▶ Smartport
 ▶ VLAN Management
 ▶ Spanning Tree
 ▶ MAC Address Tables
 ▶ Multicast
 ▶ **IP Configuration**
 ▶ IPv4 Management and Interface
 ▶ IPv4 Interface
 ▶ **IPv4 Routes**
 ▶ ARP
 ▶ ARP Proxy
 ▶ UDP Relay/IP Helper
 ▶ DHCP Snooping/Relay
 ▶ DHCP Server
 ▶ IPv6 Management and Interface
 ▶ Domain Name System
 ▶ Security
 ▶ Access Control
 ▶ Quality of Service
 ▶ SNMP

IPv4 Static Routing Table

<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Route Owner	Metric
<input type="checkbox"/>	192.168.5.0	24	Local		Directly Connected	
<input type="checkbox"/>	192.168.11.0	24	Local		Directly Connected	
<input type="checkbox"/>	192.168.12.176	29	Remote	192.168.13.253	Static	2
<input type="checkbox"/>	192.168.13.0	24	Local		Directly Connected	

Add... Add IPv4 Static Route - Profil 1 - Microsoft Edge

Non sécurisé 192.168.5.254/cs950543f4/routing/ip_rout_a.htm

Destination IP Prefix: 192.168.10.176

Mask: Network mask Prefix length 29

Route Type: Reject Remote

Next Hop Router IP Address: 192.168.11.253

Metric: 2 (Range: 1 - 255, Default: 1)

Apply Close

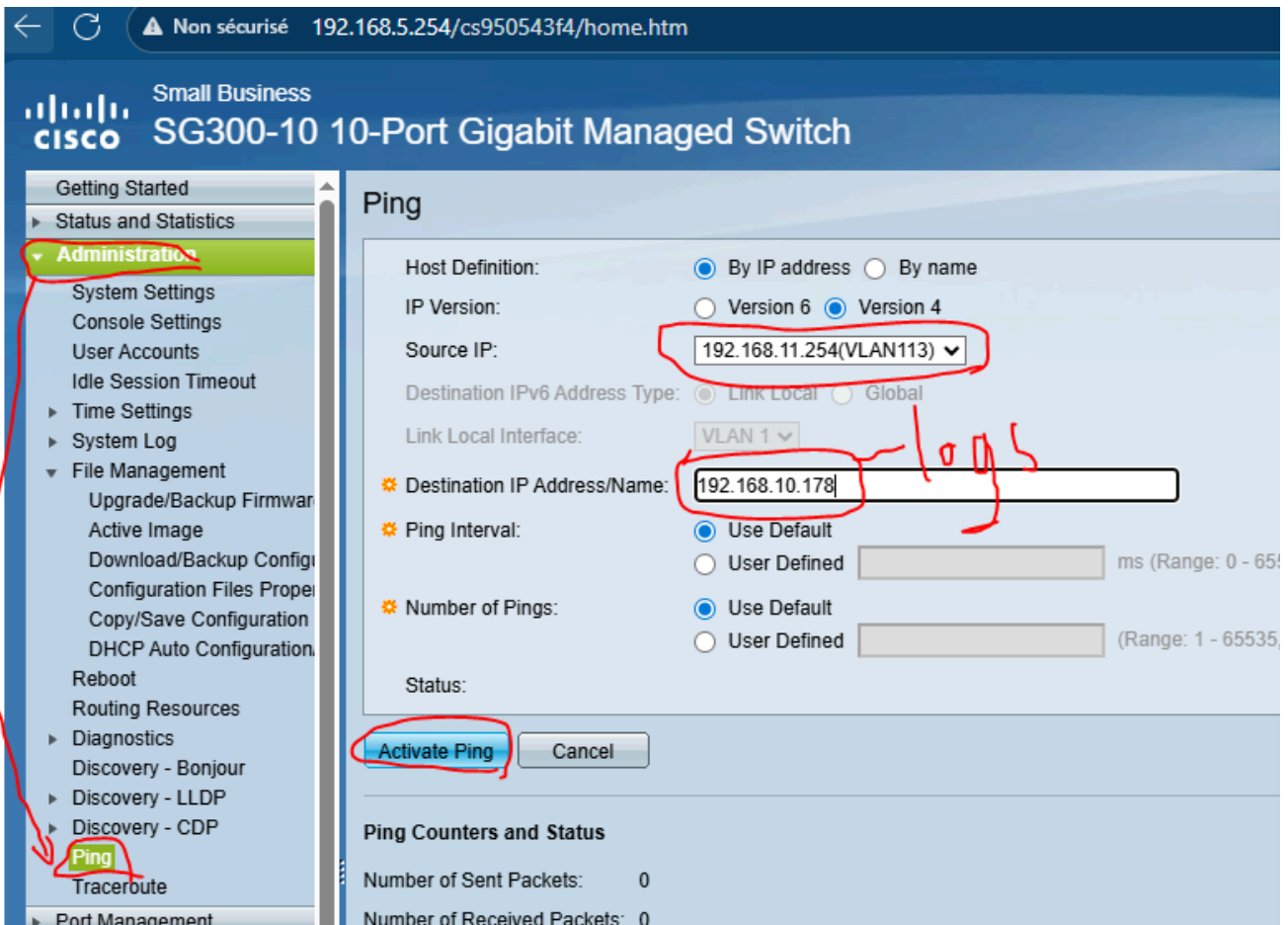
sur le sts interne
faut ajouter une regle encore

FILTORAGE NAT

Rechercher... + Nouvelle règle X Supprimer ↑ ↓ ↶ ↷ Couper Copier

	État	Action	Source	Destination	Port dest.
8	off	passer	Network_wifi	Internet	http https
9	on	passer	Network_in interface: in	Internet	* Any
10	off	bloquer	* Any	* Any	* Any
11	on	passer	Network_srv_prod interface: srv_prod	Network_srv_auth	* Any
12	on	passer	Network_client1	Network_srv_prod	* Any
13	on	passer	Network_srv_auth interface: srv_auth	Network_srv_prod	* Any
14	on	passer	Network_srv_it interface: srv_it	Network_srv_prod Network_srv_auth	* Any
15	on	passer	Network_wifi interface: wifi	srv_logs	* Any
16	on	bloquer	* Any	* Any	* Any

sur le csico
faut activer les pings pour etablir une connexion au ciscosu srv de logs



sur srv_logs
on peut voir les logs de cisco avec son ip

Time	Source	Severity	Destination	Process	Source IP	Destination IP	Message
Today 10:52:11	USER	NOTICE	sts-interne	ssh			...
Today 10:51:52	USER	NOTICE	sts-interne	ssh			...
Today 10:51:42	USER	INFO	sts-interne	asqd			...
Today 13:49:57	LOCAL6	NOTICE	192.168.11.254	COPY			%COPY-N-TRAP: The copy operation was completed successfully
Today 13:49:54	LOCAL6	INFO	192.168.11.254	COPY			%COPY-I-FILECOPY: Files Copy - source URL running-config destination URL flash:// ...
Today 10:51:05	USER	ALERT	sts-interne	asqd			...
Today 10:51:05	USER	ALERT	sts-interne	asqd			...
Today 10:51:05	USER	ALERT	sts-interne	asqd			...

sur le sts_interne
on peut voir les pings reussir entre les cisco et sr_logs

```
sts_interne_mark sur 9-RA-P2 - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
4 client2 hm3 up 192.168.10.126/26
5 wifi hm4 up 192.168.11.253/24
6 srv_prod hm5 up 192.168.10.174/28
7 srv_it hm6 up 192.168.10.182/29
8 srv_auth hm7 up 192.168.10.190/29

sts-interne-UMSNSX09K0639A9>ping 192.168.11.254
PING 192.168.11.254 (192.168.11.254): 56 data bytes
64 bytes from 192.168.11.254: icmp_seq=0 ttl=64 time=1.597 ms
64 bytes from 192.168.11.254: icmp_seq=1 ttl=64 time=1.317 ms
64 bytes from 192.168.11.254: icmp_seq=2 ttl=64 time=1.583 ms
^C
--- 192.168.11.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.317/1.499/1.597/0.129 ms
sts-interne-UMSNSX09K0639A9>ping 192.168.10.178
PING 192.168.10.178 (192.168.10.178): 56 data bytes
64 bytes from 192.168.10.178: icmp_seq=0 ttl=64 time=0.205 ms
64 bytes from 192.168.10.178: icmp_seq=1 ttl=64 time=0.222 ms
64 bytes from 192.168.10.178: icmp_seq=2 ttl=64 time=0.183 ms
^C
--- 192.168.10.178 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.183/0.203/0.222/0.016 ms
sts-interne-UMSNSX09K0639A9>
```

Conclusion

SRV de Log opérationnel.

*Log de notre Stormshield interne à notre SRV Log

Log de notre Switch Cisco à notre SRV Log