



### BTS SIO 2025 Option SISR Projet : DATATEL <u>DOCUMENTATION TECHNIQUE</u>



### **Epreuve E6**

### Situation professionnelle 2

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 1 / 197 - CHAHROUR Walid





### Table des matières

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)..... Erreur ! Signet non défini.

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)..... Erreur ! Signet non défini.

Contexte	Erreur ! Signet non défini.
Besoins et contraintes	Erreur ! Signet non défini.
Solutions retenues et argumentations	Erreur ! Signet non défini.
Schéma réseau	Erreur ! Signet non défini.
Coût du projet	Erreur ! Signet non défini.
Planning prévisionnel	Erreur ! Signet non défini.
Planning réel	Erreur ! Signet non défini.
Planning prévisionnel vs réel	Erreur ! Signet non défini.
Conclusion	Erreur ! Signet non défini.
Améliorations possibles	Erreur ! Signet non défini.



### Création, d'une VM sur VM WARE

BTSSID

Lorsque vous créer une machine virtuelle l'option « Typical (recommended) est cocher de base.







Dans notre cas à nous allons choisir « Linux » car nous auront besoin d'installer d'un pare-feu sur le serveur

	New Virtual Mach	ine Wizard	×
Cliquer dans le menu déroulant puis sélectionner « Linux»	Select a Guest Which oper	t <b>Operating System</b> ating system will be installed on this virtual machine?	
Cliquer sur « Next » pour passer à la prochaine étape	Guest operating sy Microsoft	/stem ows	
	Ubuntu	2	~
Dans cette étape nous allons devoir nommer le serveur ainsi que choisir			
New Virtual Machine Wizard			
Name the Virtual Machine What name would you like to use for this virtual machine	Help	< Back Next > Cana	
Virtual machine name:		l'emplacement de la VM	
		(1) Ensuite nous allons nommer le ser	rver
The default location can be changed at Edit > Preferences.	Broge	(2) Choisir l'emplacement ou sera situ	ué la VIV
		(3) Cliquer sur « Next » pour passer à prochaine étape	la
< Back Next >			

Ensuite sur cette étape nous allons allouer

l'espace du disque pour notre serveur. Dans notre cas il n'est pas nécessaire d'avoir un gros espace de stockage sur notre serveur.





Cliquer sur « Next » pour passer à la prochaine étape	New Virtual Machine Specify Disk Capa How large do yo	Wizard X city ou want this disk to be?	
	The virtual machine's ha physical disk. These file( files, and data to your v Maximum disk <u>si</u> ze (GB):	rd disk is stored as one or more files on the host computer's (s) start small and become larger as you add applications, irtual machine.	-
	Recommended size for U	Ibuntu: 20 GB	
	<ul> <li>Store virtual disk as a</li> <li>Split virtual disk into a</li> <li>Splitting the disk male</li> </ul>	a single file <u>m</u> ultiple files kes it easier to move the virtual machine to another computer	
Ensuite dans cette partie-là nous configurer les options suivantes :	but may reduce perf	ormance with very large disks.	allons
New Virtual Machine Wizard	×		
Ready to Create Virtual Machine Click Finish to create the virtual machine. Then you c	an install Ubuntu.	<u>A Back</u> <u>Next</u> Cancel Cliquer sur « Customize Hardware »	-
The virtual machine will be created with the following settin	gs:		
Name:     RTE-01       Location:     E:\VM\BTS-SIO\AP4\RTE-01       Version:     Workstation 17.5 or later       Operating System:     Ubuntu			
Hard Disk: 20 GB, Split Memory: 4096 MB Network Adapter: NAT Other Devices: 2 CPU cores, CD/DVD, USB Controlle	r, Sound Card		
<u>C</u> ustomize Hardware			
		Dans cette partis nous allons paramétr	er selon
< <u>B</u> ack Fin	nish Cancel		





/·· ··	Hardware	×	
<ol> <li>Memory = 4 GB</li> <li>CD/ DVD = Pfsens</li> <li>Network Adapter = Vmnet 4 Network Adapter = Vmnet 4</li> <li>Network adapter = Vmnet 1</li> <li>Cliquer sur « Close » pour fenêtre</li> </ol>	Device Summary () Device Summary () Processors 2 Chaew Ch/Du (SATA) Lising Rie C-Y Leers (Pally, T/Ch.) Content Adapter 3 Custom (Mmet4) Content Adapter 2 Custom (Mmet4) Control Card Auto detect Display Auto detect 128 64 226 226 226 226 226 226 226	ry	la
Une fois que la configuration vous aller avoir ce menu-là : New Virtual Machine Wizard <b>Ready to Create Virtual Machine</b> Click Finish to create the virtual m	Add Remove	est finit	t
The virtual machine will be created with Name: RTE-01 Location: E:\VM\BTS-SIO\A Version: Workstation 17.5 Operating System: Ubuntu Hard Disk: 20 GB, Split Memory: 4096 MB Network Adapter: Custom (VMnet4) Other Devices: 2 CPU cores, CD/ Customize Hardware	the following settings: P4\RTE-01 or later , Custom (VMnet4), Custom (VMnet1) DVD, USB Controller, Sound Card	<ul> <li>(1) Récapitulatif de la configuration du serveur.</li> <li>(2) Cliquer sur « Finish » pour passe la prochaine étape</li> </ul>	ı er à
	Finish Cancel	Une fois avoir fini de vérifier les information du serveur, la VM ( Virtual Machine) va se créer ainsi vous pouvez le lancer.	









### BTSSID Installation Pfsense

< <mark>d</mark>k >

Lorsque la machine à démarrer vous allez avoir cette interface et donc il faudra patienter quelque seconde afin que pfsense lance l'installation.

= Welcome to pfSense Boot Multi user [Enter] Boot Single user Escape to loader prompt Reboot Cons: Serial Options: Kernel: default/kernel (1 of 1) **Boot Options** Autoboot in 0 seconds. [Space] to pause Loading kernel... /boot/kernel/kernel text=0x19aae8 text=0xfe04e8 text=0x17d8e18 data=0x180 data=0 x265d28+0x3992d8 0x8+0x1c8828+0x8+0x1d4fd4-Une fois que cela est fait /boot/kernel/zfs.ko size 0x5ba0d8 at 0x359e000 /boot/kernel/zfs.ko size 0x5ba0d8 at 0x359e000 /boot/kernel/opensolaris.ko size 0xaab0 at 0x3b59000 can't find '/boot/entropy' can't find '/etc/hostid' vous allez atterrie sur cette page avec les conditions à accepter d distribution notice -Copyright and Trademark Notices. Sélectionner « Accept » Copyright(c) 2004-2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved. Copyright(c) 2014–2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved. All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate. "pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All Welcome to pfSense! [Accep Install Install pfSense aunch a shell for rescue operations Sélectionner « Install » Recover config.xml Recover config.xml from a previous install <Cancel> < <mark>d</mark>k > How would you like to partition your disk? Sélectionner « Auto (ZFS) Auto (ZFS) Guided Root-on-ZFS Guided UFS Disk Setup Manua l Manual Disk Setup (experts) Shell Open a shell and partition by hand

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 9 / 197 - CHAHROUR Walid

<Cancel>













- (2) Choix option
- (3) Zone de choix à entrer



### Assignation des interfaces sur pFsense

Une fois après avoir vu le menu nous allons assigner les interfaces

- (1) Choisir set interface IP
- (2) Renter le numéro 2 accéder à cette option
- 0) Logout (SSH only)
   9) pfTop

   1) Assign Interfaces
   10) Filter Logs

   2) Set interface(s) IP address
   11) Restart webConfigurator

   3) Reset webConfigurator password
   12) PHP shell + pfSense tools

   4) Reset to factory defaults
   13) Update from console

   5) Reboot system
   14) Enable Secure Shell (sshd)

   6) Halt system
   15) Restore recent configuration

   7) Ping host
   16) Restart PHP-FPM

   8) Shell
   2

Une fois sélectionner le bon choix merci vous allez devoir choisir entre le WAN, LAN ou OPT1. Pour nous cela être le choix 2 LAN



Une fois cela fait nous allons devoir répondre à plusieurs questions :







### **Connexion interface pfsense**

Une fois après avoir bien fixer les ip nous allons nous connecter sur l'interface Pfsense en tapant l'adresse ip indiquer sur le serveur.



- (1) Rentrer l'IP du lan qui est 192.168.10.1
- (2) Cliquer sur avancer



#### Cliquer sur Continuer vers 192.168.10.1 (non sécurisé)



#### Votre connexion n'est pas privée

Les utilisateurs malveillants essaient peut-être de voler vos informations de **192.168.10.1** (par exemple, les mots de passe, les messages ou les cartes de crédit).

NET::ERR\_CERT\_AUTHORITY\_INVALID

Masquer les éléments avancés

Après voir cliquer nous allons arriver sur le page de

	Ce serveur n'a pas pu prouver qu'il s'agit de 192.168.10.1. Son certificat de sécurité n			
<i>pf</i> sense	Login to pfSense	ar le système d'exploitation de votre ordinateur. Cela peut être dû à une correcte ou à un utilisateur malveillant qui intercepte votre connexion.		
		2.168.10.1 (non sécurisé)		
SIGN IN		connexion de Pfsense.		
Username				
Password		(1) Admin		
воч ни 🕄 3		(2) Pfsense		
		(3) Cliquer sur Signe IN pour se		
connecter				

### **Configuration depuis l'interface Web pfsense**

Une fois après être connecter sur l'interface de Pfsense vous allez être sur cette page.





COMMUNITY LOTION System - Interfaces - Firewall - Services - VPN - Sta	atus 🕶 Diagnostics 👻 Help 👻	GÞ		
WARNING: The 'admin' account password is set to the default value. Change the password in the User	r Manager.			
Wizard / pfSense Setup / Netgate® Global Support is available 2	24/7	Θ		
Step 1 of 9				
Netgate@ Global Support is available 24/7 Our 24/7 worldwide team of support engineers are the most qualified to on premises to cloud. We offer several support subscription plans tailored to fit different enviro Netgate support because: Support is available 24 hours a day, seven days a week, including Support is available 24 hours a day, seven days a week, including Support engineers are located around the world, ensuring that no Our support engineers and of any prestigious network engineer or	diagnose your issue and resolve it quickly, fr onment sizes and requirements. Many comp holidays. support call is missed. rtificates and have years of hands-on experi	om branch office to enterprise — anles around the world choose ence with networking.		
Learn more Next		(1) (2)	Mettre le nom du rout Mettre le DNS de goog	eur RTE-01 le
Community controls Community controls WARNING: The ladmin acco	<ul> <li>Interfaces          Firewall           Sound password is set to the default value. Of the set to the default value.     </li> </ul>	ervices - VPN - Status - Diagnos	tics + Help + 💽	
Wizard / pfSense	Setup / General Information	on	Θ	
Step 2 of 9				
General Information Hostname	On this screen the general pfSense para RTE-01 २७: जाउंगे: जुटरास्ट, गठार एक फ्रिट	meters will be set.		
Primary DNS Server 8.8.8.8		D		Cliquer
Secondary DNS Server				sur Next
Override DNS Allow DNS servers to be overridden by D	DHCP/PPP on WAN	he final part (Top Level Domain, TLD). The 'loca Jows systems and networked devices. These w r 'mylocal' are safe.	l' TLD is widely used by mDNS (e.g. Avahi, Bonjour, ill not network correctly if the router uses 'local' as its TLD.	
>> Next		l ignore manually configured DNS servers for cli lient queries, visit Services > DNS Resolver and	ent queries and query root DNS servers directly. To use the enable DNS Query Forwarding after completing the wizard.	
	COMMUNITY EDITION	aces → Firewall → Services → VPN →	Status ▼ Diagnostics ▼ Help ▼	0
Secondary DNS Server	WARNING: The 'admin' account passwo	rd is set to the default value. Change the password in	the User Manager.	
(1) Cliquer sur menu Override DNS	Wizard / pfSense Setup /	Time Server Information		0
déroulant et sélectionner	Step 3 of 9			
Europe/Paris	Time Server Information			
(2) Cliquer sur Next	Please ent Time server hostname 2.pfsens	e.pool.ntp.org		
	Enter the l	iosuname (FQDN) of the time server.		
	Timezone Europe/	Paris	<ul> <li>✓</li> <li><b>●</b></li> </ul>	



Dans cette partie il n'y pas grand-chose à modifier

COMMUNITY EDITION		us - Diagnostics -	Help 🕶	G	
WARNING: The 'admin' acc	count password is set to the default value. Change the password in the User I	Manager.			
Wizard / pfSense	e Setup / Configure WAN Interface			0	
Configure WAN Inter	Step 4 of 9				Pas d'élément à modifier
	On this screen the Wide Area Network information will be configured.				
SelectedType	DHCP				
General configuratio	n 				
мти	This field can be used to modify ("spoot") the MAC address of the WAN in in the following format: xxxxxxxxxxxxx or leave blank.	terface (may be required wit	h some cable connections) Static IP Configuratio	n. Enter a MAC address	
	Set the MTU of the WAN interface. If this field is left blank, an MTU of 149 assumed.	2 bytes for PPPoE and 1500	IP Address Subnet Mask	32	۲.
MSS	If a value is entered in this field, then MSS clamping for TCP connections this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes fo MTU value in most all cases.	to the value entered above m r all other connection types v	Upstream Gateway	ation	
			DHCP Hostname	The value in this field is identification).	sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client
			PPPoE configuration		
			PPPoE Osemanie PPPoE Password		
Pas d'élém	ent à modifier		Show PPPoE password	<ul> <li>Reveal password ch</li> </ul>	aracters
			PPPoE Service name		
			PPPoE Dial on demand	Hint: this field can usua	Ily be left empty and mode
PPTP configuration				This option causes the	interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual s delayed until qualifying outgoing traffic is detected.
PPTP Username					
PPTP Password				1	g packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables
Show PPTP password	Reveal password characters				
PPTP Local IP Address					(1) Décocher la case Block private
pptplocalsubnet	32 🗸				networks from entering via WAN
PPTP Remote IP Address					(2) Décesher la case Plack pon
PPTP Dial on demand	<ul> <li>Enable Dial-On-Demand mode</li> <li>This option causes the interface to operate in dial-on-demand mode, allowi connection of the link is delayed until qualifying outgoing traffic is detected</li> </ul>	ing a virtual full time connecti I.	tion. The interface is configu	ured, but the actual	Internet routed netdwork from entering
PPTP Idle timeout	If no qualifying outgoing packets are transmitted for the specified number of the fortune of the specified number of the fortune of the specified number of the specified numb	of seconds, the connection is	s brought down. An idle time	eout of zero disables	via WAN (3) Cliquer sur Next
RFC1918 Networks	inis reature.				
Block RFC1918 Private Networks	Block private networks from entering via WAN     When set, this option blocks traffic from IP addresses that are reserved for     loopback addresses (127/8). This option should generally be left turned on	private networks as per RFC , unless the WAN network lie:	: 1918 (10/8, 172.16/12, 192 is in such a private address	2.168/16) as well as space, too.	
Block bogon network	\$				
Block bogon networks	Block non-Internet routed networks from entering via WAN     When set, this option blocks traffic from IP addresses that are reserved (bus should never appear in the Internet routing table, and obviously should not	it not RFC 1918) or not yet as appear as the source addres:	ssigned by IANA. Bogons ar is in any packets received.	e prefixes that	
	>> Next		m ← Interfaces ←	Firewall 🗸 Ser	vices • VPN • Status • Diagnostics • Help •
		WARNING: The 'admin' ad	ccount password is set to	the default value. Cha	nge the password in the User Manager.
(1) Vér	ifier bien que les				
(_, info	rmation soit hon	Wizard / pfSens	se Setup / Config	gure LAN Inter	face
(2) Clia	uer eur Novt		Step 5 o	of 9	
	UCI SUI INEXL	Configure LAN Inte	on this screen the Lo	ocal Area Network info	rmation will be configured.
		LAN IP Address	192.168.10.1 Type dhcp if this inte	rface uses DHCP to ol	stain its IP address.
		Subnet Mask	24		•]
			>> Next	2	

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 16 / 197 - CHAHROUR Walid



	System <del>-</del>	Interfaces 👻	Firewall 🗸	Services -	VPN <del>-</del>	Status 🗸	Diagnostics 👻	Help 🗸	G <del>)</del>
WARNING: The 'a	admin' account	password is set to	the default value.	. Change the pa	ssword in the	e User Manager			
Wizard / p	fSense Se	etup / Set A	dmin WebG	UI Passwo	ord				0
			Step 6 of 9						
Set Admin W	ebGUI Pass	word							
	Or	n this screen the ac	lmin password wi	ll be set, which i	s used to acc	cess the WebGl	UI and also SSH serv	rices if enabled.	
Admin Pa	assword								
Admin Password									
	(	» Next							

- (1) Mettre en place le mot de passe Testap04@
- (2) Cliquer sur Next

Une fois après modifier le mot de passe nous allons redémarrer la configuration





#### Après avoir cliquer sur Close comme vous pouvez le voir la configuration de l'interface de pFsense est

Status / Da	BIIDUalu	÷ (
System Inforn Name	nation $ earrow  earro$	Netgate Services And Support
Jser	admin@192.168.10.3 (Local Database)	Community Support Only
System	VMware Virtual Machine Netgate Device ID: <b>c0c2e14b1cb2149bf18a</b>	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
BIOS	Vendor: <b>Phoenix Technologies LTD</b> Version: <b>6.00</b> Release Date: <b>Thu Nov 12 2020</b>	If you purchased your pfSense gateway firewall appliance from Netgate and electer
/ersion	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT Version 2.7.2 is available. Version information updated at Sun Mar 16 16:52:57 CET 2025	hardware, you have access to various community support resources. This includes the <b>NETGATE RESOURCE LIBRARY</b> . You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
СРU Туре	AMD Ryzen 5 5600X 6-Core Processor 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	• Upgrade Your Support         • Community Support Resources           • Netgate Global Support FAQ         • Official pfSense Training by Netgate           • Netgate Professional Services         • Visit Netgate.com
lardware crypto	Inactive	
ernel PTI	Disabled	If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to
IDS Mitigation	Inactive	validate support for this unit. Write down your NDI and store it in a safe place.
Jptime	01 Hour 55 Minutes 40 Seconds	rou can purchase TAC supports nere.

bien fini

### **Création du CARP dans Pfsense**

Nous allons créer un carp sur le routeur pour cela nous allons cliquer dans le menu de la barre de pfsense







Puis ensuite refaire la même métode avec le LAN

BTSSID

Encoded A Material Day 4 Ente		0	(1)	Cocher la case CARP	
Firewaii / Virtual IPS / Eult		U	(2)	Rentrer l'ip 192.168.10.10	
Edit Virtual IP Type OIP Alias CARP OPPOR	v ARP Other		(3)	Rentrer un mot de mot de pass	se
Interface LAN	2				
Address type Single address ~	, -				
Address(es) 192.168.10.10		/ 24 ~ 3			
The mask must be the network's subnet mask. It does not specify a CIDR	range.				
Virtual IP Password Enter the VHID group password.					
VHID Group 2 Fater the MUD group that the machines will share	VHID Group	2 Enter the VHID group that the	machines will sha	are.	
Advertising frequency 1	Advertising frequency	1		~	<b>~</b>
(1) Rentrer une description		Base		Skew	
(2) Cliquer sur Save		The frequency that this machin master.	ne will advertise.	0 means usually master. Otherwise the lowest combination of both values in the second se	the cluster determines the
(2) Cliquel sul Save	Description	LAN IP virtual			
		A description may be entered l	here for administ	rative reference (not parsed).	
		Save 2			
				Cliquer sur Apply Chang	ge
The VIP configuration has been changed.			Apply	Changes	
The changes must be applied for them to take effect.					
Message de confirmation			The	changes have been applied suc	cessfully
			The	changes have been applied suc	cessfully.
The changes have been applied successfully.				×	
Virtual IP Address					
Virtual IP address	Interface	Туре	Descriptio	on Actions	
192.168.1.100/24 (vhid: 1)	WAN	CARP	WAN Virt	tual IP 🧳 🛅	
192.168.10.10/24 (vhid: 2)	LAN	CARP	LAN IP vi	irtual 🥒 🛅	
				Add	

Une fois voici le résultat





(3) Rentrer l'ip du routeur 2 su LAN : 192.168.10.2



(1)Rentrer l'ip du routeur(2)Rrentrer le nom utilisateur(3)Rentrer le mot de passe pour se connecter au pfsense





- (1) Cliquer sur Toogle all pour tout selectionner les option
- (2) Cliquer sur Save

Select options to sync	User manager users and groups
	Authentication servers (e.g. LDAP, RADIUS)
	Certificate Authorities, Certificates, and Certificate Revocation Lists
	Firewall rules
	Firewall schedules
	Firewall aliases
	NAT configuration
	IPsec configuration
	OpenVPN configuration (Implies CA/Cert/CRL Sync)
	DHCP Server settings
	DHCP Relay settings
	DHCPv6 Relay settings
	WoL Server settings
	Static Route configuration
	Virtual IPs
	Traffic Shaper configuration
	Traffic Shaper Limiters configuration
	DNS Forwarder and DNS Resolver configurations
	Captive Portal

### **Règle pare-feu Pfsyncs**



### **Confuguration double WAN**

Pour configurer le double WAN depuis l'interface web nous allons devoir cliquer dans une catégorie

System -	lfaces	vices → VPN → Status →	• Diagnostics ▼ Help	(1)	Cliquer	sur System	
Certificates General Setup High Availability Package Manager Register Routing Setup Wizard Update User Manager Logout (admin) built on Wed Jun 2	: (Local Database) ine c2e14b1cb2149bf18a mologies LTD v 12 2020 64) 28703:53:34 UTC 2023	Image: Second system       Netgate S         Co       Co         If you purcha       Community         If you purcha       Community         If second system       System	ervices And Support ntract type Community Supp Community Supp TGATE AND pfSense COMMU ased your pfSense gateway fire Support at the point of sale or m - Interfaces - Firewall -	(Ζ) port port Oni UNITY S wall app installe Services - VF	Cirquer <sup>•</sup> N • Status •	Diagnostice + Help +	C+
ne vous po ue un WAN	ouvez le voir no N	System / Routin US Gateways Name © WAN_DHCP ( Default gateway IPvd Default gateway IPvd	Ing / Gateways  toutes Gateway Groups  Default Interface  WAN  Automatic Select a gateway or failover gate  Automatic Select a gateway or failover gate  Automatic	Gateway 192.168.1.254 way group to use as the d	Monitor IP 192.168.1.254	Description Interface WAN_DHCP Gateway	Actions
tre cas nou er une deu	us allons uxième interfac	ce o	Select a gateway or failover gate	way group to use as the o	erauit gateway.		
em / Rout	em • Interfaces • ing / Routes Routes	F (1) (2) (2)	Cliquer sur Cliquer sur	Interface Assignem	ents		
	Advanced Certificates General Setup High Availability Package Manager Register Routing (2) Setup Wizard Update User Manager Logout (admin) built on Wed Jun 2 De VOUS PC Le UN WAN	Advanced Certificates General Setup High Availability Package Manager Register Register Register Reduting Setup Wizard Update User Manager User Manager User Manager v 12 2020 Logout (admin) built on Wed Jun 28 03:53:34 UTC 2023 The vous pouvez le voir nor the vous pouvez le voir nor the vous pouvez le voir nor the un WAN the cas nous allons er une deuxième interfaces em / Routing / ays Static Routes Prewal * Set Prewal * Static Routes Prewal * Static Routes	Advanced Certificates General Setup High Availability Package Manager Register (Local Database) Ine c2a14b1cb2149bf18a welogies LTD Ugdate User Manager Logout (admin) built on Wed Jun 28 03:53:34 UTC 2023 Mane Community Gateways System / Routi Community System / Routi Community Default gateway Pre- Default	Advanced       Certificates       General Setup       Netgate Services And Support         High Availability	(1) (2) Advanced Certificates General Step High Availability Peckage Manager Regiser Contract type Contract type Con	Advanced       Cliquer       (1)       Cliquer         Advanced       Certification       (1)       Cliquer         (2)       Cliquer       (2)       Community Support Cliquer         (2)       Cliquer       (2)       State       State         (2)       Cliquer       (2)       State       State         (2)       Cliquer       State       State       State         (2)       State       State       State </td <td>Within a link of the service with link of the service with a link of the service with a link of th</td>	Within a link of the service with link of the service with a link of the service with a link of th

#### Une fois sur l'interface vous allez voir plusieurs carte réseaux

Interfaces / Interface Assignments											
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs		
Interface	Network por	t									
WAN	le0 (00:0c:	29:83:39:8d)						~			
LAN	le1 (00:0c:	29:83:39:97)						~	Delete		
OPT1	le2 (00:0c:	29:83:39:a1)						~	Delete		
R Save											

Cliquer sur OPT1





		Interfaces / OPT	1 (le2)	<b>≠ ⊎ 0</b>
(1) Cocł	ner la case enable	General Configuration	n	
inter	rface	Enable	Enable interface	
(2) Mod	lfiier la description par	Description	WAN2 Enter a description (name) for the interface her	2 re.
WAN	N 2	IPv4 Configuration Type	DHCP	3
(3) Cliqu	uer sur le menu déroulant	IPv6 Configuration Type	None	v)
et ch	noisir DHCP	MAC Address	xxxxxxxxx This field can be used to modify ("spoof") the N Enter a MAC address in the following format: x	AAC address of this interface. xxxxxxxxxxxx or leave blank.
		MTU	If this field is blank, the adapter's default MTU v	will be used. This is typically 1500 bytes but can vary in some circumstances.
dans cette p	partis là rien est à	MSS	If a value is entered in this field, then MSS clam minus 60 for IPv6 (TCP/IPv6 header size) will b	nping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and se in effect.
toucner	www.windo. Moo r be set to autoselect (automatically negotiate speed) o	niess the Sored and Onales co	nne Sisfa: Ha's no spleearana taipel: rardealo-+)	~
DHCP Client Configu	ration			rface. ally negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Options	Advanced Configuration	Configuration Overrid	le	
	Use advanced DHCP configuration options.	Override the configuratio	on from this file.	
nostiane	The value in this field is sent as the DHCP client identifier and hostname identification).	e when requesting a DHCP lease	e. Some ISPs may require this (for client	
Alias IPv4 address	The value in this field is used as a fixed alias IPv4 address by the DHCP	client.	/ 32 ~	Cliquer sur save
Reject leases from	To have the DHCP client reject offers from specific DHCP servers, enter for rejecting leases from cable moderns that offer private IP addresses	their IP addresses here (separa when they lose upstream sync.	ate multiple entries with a comma). This is useful	
Reserved Networks				1
Block private networks and loopback addresses	Blocks traffic from IP addresses that are reserved for private networks RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option private address space, too.	per RFC 1918 (10/8, 172.16/12, should generally be turned on,	,192.168/16) and unique local addresses per unless this network interface resides in such a	
Block bogon networks	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet routing table, and so should not appear as the source address in any pa This option should only be used on external interfaces (WANs), it is not Note: The update frequency can be changed under System > Advanced,	assigned by IANA. Bogons are okets received necessi Firewal	prefixes that should never appear in the Internet	
	R Save	interfaces /	WANZ (ICZ)	÷ 🕮 🔮
		The WAN2 configura The changes must b Don't forget to adjus	ation has been changed. Je applied to take effect. It the DHCP Server range if needed after applying.	Apply Changes
Cliquer sur .	Apply Changes	a 10 (*		

Ensuite un message s'affiche pour vous dire que la configuration à bien était prise en compte



Puis pour bien voir si le WAN 2 est bien actif nous allons allez dans le menu suivant :







(2) Cliquer sur Interfaces

		s 👻 VPN	• St		
			С	aptive Portal	
			С	ARP (failover)	
			D	ashboard	
			D	HCP Leases	
			D	HCPv6 Leases	
			D	NS Resolver	_
			— Fi	ilter Reload	
Disense Susta	n y Interfacency Firewall y Consider y UDN y Status y Disconstition y Hole y	e.	G	ateways	_
COMMUNITY EDITION	n interaces interail defices fin datas playnoside inter		In	nterfaces 2	
Status / Interfa	ces	≢ ⊡ 😧	IF	osec	
Status DHCP MAC Address IPv4 Address Subnet mask IPv4 Qateway IPv4 IPv6 Link Local IPv6 Address Subnet mask IPv6 DNS servers MrTU Media In/out packets (back) In/out packets (back) In/out packets (back) In/out packets (back) In/out packets (back) In/out packets (back) In/out packets (back)	up ↑ C Reserve WAN 000c2:98339.84 102163.128 255255.255.0 102163.128 255255.255.0 2001861.366.526.02.0c29ff.fe83.398d 64 192.168.1254 1050 autoselect 38422/38706 (15.24 MB/1.70 MB) 38422/38706 (15.24 MB/1.70 MB) 38420 (15.24 MB/1.70 MB/1.70 MB) 38420 (15.24 MB/1.70 MB/1.70 MB) 38420 (15.24 MB/1.70 MB/1.70 MB/1.70 MB) 38420 (15.24 MB/1.70 MB/1.7		Desce	endre jusqu'à	a voir le WAN 2
LAN Interface (lan,	le1)	WAN2 Int	ertace (o Status	pt1, le2)	
Status MAC Address IPv4 Address Subnet mask IPv4 IPv6 Link Local	up <b>1</b> 00.0c 29.8339.97 192.168.10.1 255.255.255.255.0 fe80::20c.29ff.683.3997%Je1 1500	M/ IP	DHCP AC Address v4 Address	up C Release WAN2 00:0c:29:83:39:a1 192.168.1.175	🗆 Relinquish Lease
Mito Media In/out packets In/out packets (pass) In/out packets (block) In/out errors	autoselect 12602/12268 (1.16 MIB/3.77 MIB) 12602/12268 (1.16 MIB/3.77 MIB) 694/16 (54 KIB/18 KIB) 0/0	Subnet Ga IPv6 D	mask IPv4 teway IPv4 Link Local NS servers	255.255.255.0 192.168.1.254 fe80::20c:29ff:fe83:39 192.168.1.254	a1%le2
Comme v	ous le voir le WAN à bien récupérer une IP	In/out pac	MTU Media out packets kets (pass)	1500 autoselect 1/5 (128 B/416 B) 1/5 (128 B/416 B)	
		In/out pack Ir	tets (block) n/out errors Collisions	17/0 (2 KiB/0 B) 0/0 0	

ET donc pour vérifier que le WAN 2 fonctionne bien nous allons aller dans le menu suivant :



•	Diagnostics -	(1) (2)	Cliquer sur Diagno Ping	ostics	
	ARP Table				
	Authentication				
_	Backup & Restore				
	Command Prompt				
	DNS Lookup				
	Edit File				
	Factory Defaults				
	Halt System				
	Limiter Info				
	NDP Table		Diagnostico / Dir		
	Packet Capture		Diagnostics / Pin	lg	
	pfInfo		Ping		
	pfTop		IP Protocol		
с.	Ping 2		Source address		
	(1) Rentrer le serveur goo	gle		VANZ Celect source address for the ping.	2
	(2) Mettre la sources c'es	t-à-dire	Maximum number of pings	3 v Select the maximum number of pings.	le WAN 2
	(3) Cliquer sur PING		Seconds between pings	1 v Select the number of seconds to wait between pings.	
				Ping 3	

comme vous pouvez le voir le WAN 2 fonctionne bien



Résultat du ping 8.8.8.8 vers le WAN2

### **Configuration un**

### groupe de passerelle

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 26 / 197 - CHAHROUR Walid



Donc pour cela nous allons retourner dans menu système puis routing

- (1) Cliquer sur System
- (2) Cliquer sur Routing



Une fois sur cette interface nous allons cliquer sur un paramètre bien précis

Syste	m / Routing	/ Gateways	5					C'® 🖿 🗉 🔞	sur un paramètre bien précis
Gatewa	rs Static Route	Gateway G	Groups						
Gatew	iys								
	Name	Default	Interface	Gateway	Monitor IP	Description		Actions	Cliquer Cateway Craups
$\odot$	WAN_DHCP		WAN	192.168.1.254	192.168.1.254	Interface WAN_	DHCP Gateway	ø 🖸	Cliquer Galeway Groups
$\odot$	WAN2_DHCP		WAN2	192.168.1.254	192.168.1.254	Interface WAN2	_DHCP Gateway	ø 📮	
								Save 🕂 Add	
Defaul	t gateway								
Defa	ilt gateway IPv4	Automatic			~				
		Select a gateway	or failover gate	eway group to use as the	e default gateway.				
Defa	ilt gateway IPv6	Automatic			~				
		Select a gateway	or failover gate	eway group to use as the	e default gateway.				
		D Same							
		B Save							
						System /	Routing /	Gateway Group	ps 🔟 🗏 😧
Clic	luer su	ır Add				Gateways	Static Routes	Gateway Groups	
									-
						Gateway G	roups		
						Group Name		Gateways	Priority Description Actions
						0			



System / Routing	/ Gateway Groups / Ed	it				幸 📖 🗐 😯	(1) (2)	Donner un nom pour le Mettre en priorité le ty	groupe pe de carte
Group Name	DUALWAN_Failover			1			qu'on	souhaite utiliser	
Gateway Priority Link Priority Virtual IP	WAN_DHCP Tier 1 WAN2_DHCP Tier 2 Gateway Tier The priority selected here defines in unnti all links in the priority will be exl used. The virtual IP field selects which (vin	vi what order failover and bala hausted. If all links in a priori tual) IP should be used wher	Interface Address Interface Address rtual IP ncing of links will b ty level are exhaus n this group applies	v     be done. M sted then th s to a local	Interface WAN_DHCP Gateway Interface WAN2_DHCP Gatewa Description Utipje links of the same priority we next available link(s) in the ner Dynamic DNS, IPsec or OpenVP	y will balance connections at priority level will be N endpoint.	(3) (4)	Réaliser une description Cliquer sur Save	١
Trigger Level	Member Down When to trigger exclusion of a memb	ber	~	Syste	m / Routing / Gatew	vay Groups			Let 🗐 😧
Description	FAILOVER WAN 1 -> WAN2 A description may be entered here fo	or administrative reference (r	anot parsed).	The gate The char	way configuration has been char nges must be applied for them to	iged. take effect.			Apply Changes
Cliquer sur Apply Change pour				Gateway Gatewa Group Nar DUALWAI	ys Static Routes Gate	Gateways	Priority Tier 1	Description FAILOVER WAN 1 -> WAN2	Actions
-0						WAN2_DHCP	Tier 2		

Une fois que vous avez appliqué les paramètre un message va apparaitre

The changes have been applied successfully.

Ceci est un message comme quoi la configuration à bien pris en compte

### Appliquer le groupe aux règles par Pare-feu

Pour cela nous allons cliquer dans le menu de la barre puis cliquer dans l'onglet suivant :

- (1) Cliquer sur Firewall
- (2) Cliquer Rules





ire	wall / Rule	es/LAN	1								≢ 📖 🗏 🕄
Floati	ng WAN	LAN	WAN2	1							
ure	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
~	6/5.74 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	۵
~	0/15 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	ી⊘⊡⊘≣×
•	• 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	҈∜₽́О́а́×
									Add ]	Add 🛅 Delete 🚫 Toggle [ Copy	🕞 Save 🕂 Separat

(1) Cliquer sur LAN(2) Ensuite cliquer sur le crayon sur la ligne LAN.NET IPV4

#### Après avoir cliqué sur le crayon vous aurez cette page

COMMUNITY EDITION	✓ Interfaces ✓ F	Firewall ▼ Services ▼	VPN ▼ Status ▼ Diagnost	cs • Help • 🕑	*
Firewall / Rules /	Edit			≢ Ш 🗏 😧	
Edit Firewall Rule					
Action	Pass Choose what to do with Hint: the difference betv whereas with block the	packets that match the crite veen block and reject is that packet is dropped silently. Ir	v aria specified below. with reject, a packet (TCP RST or ICMP p either case, the original packet is discard	ort unreachable for UDP) is returned to the sender, led.	Descendre jusqu'à voir la section Extra
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable</li> </ul>	e this rule without removing	it from the list.		
Interface	LAN Choose the interface fro	om which packets must com	► to match this rule.		
Address Family	IPv4 Select the Internet Proto	ocol version this rule applies	<b>∨</b> to.		
Protocol	Any Choose which IP protoc	ol this rule should match.	~		
Source			Extra Options		
Source Destination	Invert match	LAN net	Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logg the Status: System Logs: Settings page).	ing for everything. If doing a lot of logging, consider using a remote syslog server (see
<u>Destination</u> Extra Options	Invert match	any	Description	Default allow LAN to any rule A description may be entered here for administrative reference log.	. A maximum of 52 characters will be used in the ruleset and displayed in the firewall
Log	Log packets that are Hint: the firewall has lim	handled by this rule	Advanced Options	Display Advanced	
Cliquer sur D	isplay Adva	anced		B Save	



Advanced Options										
Source OS	Any									
	Note: this only works for TCP rules. General OS choice matches all subtypes.									
Diffeens Code Deint										
Diffaely code Folik	¥									
Allow IP options	Allow packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.									
Disable reply-to	) Disable auto generated reply-to for this rule.									
Tag										
	A packet matching this rule can be marked and this mark used to match on other NAT/filter rules. It is called <b>Policy filtering</b>									
Tagged	Invert     Tagged									
	Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.									
Maria and a										
Max. states										
	Maximum state entries this rule can create.									
Max. src nodes										
	Maximum number of unique source hosts.									
May connections										
max. connections										
	Maximum number of established connections per nost (TCP only).									
Max. src. states										
	Maximum state entries per host.									
Maria and Data										
max. src. conn. Rate										
	Maximum new connections per host (TCP only).									

#### Descendre jusqu'à voir l'option Gateway

#### Après avoir trouver l'option en question

- (1) repérer Gatway
- (2) Cliquer sur le menu déroulant
- (3) Sélectionner DUAL WAN FAILOVER

Gateway	Default	<b>v</b> 2
1	Default WAN_DHCP - 192.168.1.254 - Interface WAN_DHCP Gateway	utilize p
In / Out pipe	DUALWAN_Failover - FAILOVER WAN 1 -> WAN2	n

Après avoir fait ceci nous allons enregistrer la configuration que nous avons effectué

Gateway	DUALWAN_Failover - FAILOVER WAN 1> WAN2	~											
	Leave as 'default' to use the system routing table. Or choose a gatewa Gateway selection is not valid for "IPV4+IPV6" address family.	iy to utili	ize policy bi	sed routing.						Clic	auer su	r Save	
ı / Out pipe	none	~	none							~	1		
	Choose the Out queue/Virtual interface only if In is also selected. The the In selection is applied to traffic coming into the chosen interface. If creating a floating rule, if the direction is In then the same rules app for outgoing.	Out sele y, if the	ection is ap direction is	lied to traffic Out the select	leaving th ions are r	ie interfac eversed, (	e whe	ere the rule is for incoming	create and Ir	ed, n is			
ue / Queue	none	~	none							~			
	Choose the Acknowledge Queue only if there is a selected Queue.												
	Save												
	Cliquer sur Apply Change		The fire The ch	wall rule configu nges must be ap	ration has t	been chang Iem to take	ed. effect.						Apply Changes
			Floatin	WAN	LAN	WAN2							
				States	Protocol	Source	Port	Destination	Port	Gateway	Queue Schedule	Description	Actions
			~	3/5.85 MiB	*	*	*	LAN Address	443 80	*	*	Anti-Lockout Rule	٥
			• •	0/15 KiB	IPv4 *	LAN net	*	*	*	DUALWAN_Failover	none	Default allow LAN to any rule	҄ѽ <i>ҝ</i> ҄҄҄҄©Ѻӓ҄×
Une f	ois avoir cliquer un messag	е	• •	0/0 B	IPv6 *	LAN net	*	*	*	•	none	Default allow LAN IPv6 to any rule	∜₽́©⊘ā×
confi	rme la configuration réalise	r									1 Add 1 Add	Toggle Copy	🖬 Save 🕂 Separato

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 30 / 197 - CHAHROUR Walid





### Test du Dual-WAN

Pour voir si tout fonctionne correctement nous allons cliquer dans le menu suivant :

(1) Cliquer sur Interfaces Interfaces -The ewa (2) WAN Assignments WAN LAN WAN2 in *of*isense 00 160 10 0 (Level Detelever) Cocher la Interfaces / WAN (le0) ≢ 📖 😧 case Enable Interface pour la General Configuration désactiver Enable Enable interface Description WAN Enter a description (name) for the interface he IPv4 Configuration Type DHCP IPv6 Configuration Type None ~ DHCP Client Configuration Advanced Configu Optic Configuration Override Override the configuration f Descendre jusqu'à trouver le bouton Save Cliquer sur Save Alias IPv4 addres / 32 te: The u Save Cliquer sur Apply Change Interfaces / WAN (le0) **≞ ⊡ 0** get to adjust the DHCP Server range if needed after applying General Configuration Enable 🗌 Enable interface Ensuite lorsque vous aurez juste

appliquer vous allez devoir allez dans la barre de menu de pfsense

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 31 / 197 - CHAHROUR Walid





Donc lorsqu'on reconnecte le WAN donc pour cela nous allons retourner sur l'interface



Cliquer sur Interfaces WAN

- (1) Cliquer sur la case pour réactiver l'interface WAN
- (2) Message de prise en compte

Interfaces / WAN	l (le0)	≢ ⊡ 🕄
The changes have been ap	plied successfully.	×
General Configuratio	n	
Enable	Z Enable interface	
Description	WAN Enter a description (name) for the interface here.	
IPv4 Configuration Type	DHCP v	
IPv6 Configuration Type	None	
MAC Address		

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 32 / 197 - CHAHROUR Walid



Ensuite pour vérifier que cela fonction nous allons retourner dans la barre du menu de pfsense

Status <del>-</del>	1	gnostics	(1) (2)	Cliqu Cliqu	ier sur ier sur	Status Gatev	s vay		
Captive Po	ortal								
CARP (fail	over)								
Dashboar	d								
DHCP Lea	ses								
DHCPv6 L	eases								
DNS Reso	lver								
Filter Relo	ad		ET d	onc co	omme	vous	pouvez le const	tater le WAI	N est bien réapparu.
Gateways Gateway Gro Gateways	ups								Pour dire que cela fonctionne bien
Yame G	ateway	Monitor	RTT	RTTsd	Loss	Status	Description	Action	
WAN_DHCP (default) 1	92.168.1.254	192.168.1.254	0.773ms	0.143ms	0.0%	Online	Interface WAN_DHCP Gateway	⊗⊗×	
WAN2_DHCP 1	92.168.1.254		Pending	Pending	Pending	Pending	Interface WAN2_DHCP Gateway	y 🙁 🗵	



### **Configuration DMZ**

Avant de configurer la DMZ, vérifier bien que vous avez une carte réseau qui est dédier. Une fois fait (1) Cliquer sur Interface

Cliquer sur OPT2

Interfaces -	(2)
Affectations	
WAN	
LAN	
WAN2	
OPT2 2	1.

Activation de l'interface L'option "Enable interface" est cochée afin d'activer l'interface réseau.

Cette étape est obligatoire pour que l'interface soit prise en compte par le pare-feu pfSense.

2. Nom de l'interface

Le champ "Description" est

renseigné avec le nom "DMZ".

Ce nom permet une identification rapide de l'interface dans les différents menus de configuration et de gestion (interfaces, règles firewall, routage, etc.).

Définir manuellement une adresse IP pour l'interface DMZ afin de l'intégrer dans un sous-réseau spécifique, ici dédié aux services placés en zone démilitarisée.





## BTSSIO

<ul> <li>IPv4 Address</li> <li>IPv4 Address</li> <li>IPv4 Listers</li> <li>IPv4 Upstream gateway</li> <li>If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.</li> <li>Reserved Networks</li> <li>Block private networks</li> <li>Block traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172,16/12, 192,168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.</li> <li>Block bogon networks</li> <li>Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.</li> </ul>	Static IPV4 Configura	tion	1 Adros
Pv4 Upstream gateway       None       IPv4 si         If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.       IPv4 si         On local area network interfaces the upstream gateway should be "none".       Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.       IPv4 si         Gateways can be managed by clicking here.       Gateways can be managed by clicking here.       IPv4 si         Block private networks       Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.       avec         Block bogon networks       Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.       avec	1 IPv4 Address	192.168.20.251 / 24 💙	1. Adress
Reserved Networks       Image: Constraint of the image:	Pv4 Upstream gateway	None Add a new gateway If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.	IPv4 stat • Le ch "IPv4 Address'
Block private networks d loopback addresses Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too. Block bogon networks Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.	eserved Networks		renseign
Block bogon networks Discussion D	Block private networks nd loopback addresses	D Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.	avec
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.	Block bogon networks	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.	

#### 192.168.20.251/24.

Cette adresse correspond à la passerelle (gateway) du sous-réseau DMZ. Elle sera utilisée comme point d'accès pour les machines situées dans la zone DMZ (exemple : un serveur web en 192.168.20.10).

#### 2. Options des réseaux réservés (à laisser décochées dans ce cas)

- "Block private networks and loopback addresses" : cette option est décochée car cette interface est destinée à une DMZ, donc un réseau privé. Activer cette option bloquerait potentiellement tout le trafic utile.
- "Block bogon networks" : décochée également, pour éviter de bloquer des plages d'adresses • utilisées localement qui ne sont pas encore officiellement allouées. Cette option est surtout utile sur une interface WAN.

#### 3. Sauvegarde de la configuration

Cliquer sur "Save" pour valider les paramètres appliqués à cette interface.

#### Importance de cette configuration :

- L'attribution manuelle d'une IP sur l'interface DMZ permet un meilleur contrôle du routage et de • la sécurité réseau.
- En DMZ, il est essentiel d'avoir une configuration réseau maîtrisée, stable et isolée du reste du réseau interne.



### **Configuration OPNVPN ROAD WARRIOR**

Création du Certifcat

Dans cette partie nous allons configurer open VPN donc pour cela nous nous diriger vers la barre de navigation de pfsense

- (1) Cliquer sur System
- (2) Cliquer sur Certificates

Cette page permet de consulter les autorités de certification déjà créées dans pfSense. Pour démarrer la configuration VPN, il faut d'abord créer une CA qui servira à signer les certificats.

Authorities	Certificates	Revocation						
Search								•
Search term				Both	~	Q Search 🕤 G	lear	
		Enter a search string or *	nix regular expression to se	arch certificate names and distinguished na	mes.			
Certificate	Authorities							
Name	Internal	Issuer	Certificates	Distinguished Name		In Use	Actions	
								+ Add

Cliquer sur **Add** pour commencer la création d'une nouvelle CA.

Dans cette vue, on configure les **premiers paramètres** de la nouvelle

autorité de certification.

- **Descriptive name** : nom lisible de la CA dans l'interface pfSense. Il doit être clair pour identifier l'usage prévu (ex : OpenVPN-CA).
- Method : permet de définir si la CA est :
  - o générée localement (Create an internal Certificate Authority),
  - o importée depuis une autre instance (externe),
  - o ou une CA intermédiaire.
- **Trust Store (optionnel)** : permet d'ajouter la CA au magasin de certificats du système pour qu'elle soit reconnue comme de confiance.
- **Randomize Serial** : génère des numéros de série aléatoires pour les certificats signés, ce qui améliore la sécurité contre les collisions ou les attaques ciblées.






Rentrer le nom souhaiter dans le Descriptive name dans notre cas ç nous c'est OpenVPN-CA

Dans cette section, on définit les détails techniques et d'identification de la CA :

- Key Type / Length : RSA 2048 bits (standard recommandé).
- Digest Algorithm : SHA256.
- Lifetime : durée de validité de la CA (ex : 3650 jours = 10 ans).
- Common Name, Organization, etc. : ces champs identifient la CA dans les certificats.

ernal Certificate #	Authority		
Key type	RSA 🗸		
	20.49		(1) Rentrer les champs demander
	The length to use when generating a new DCA key in hits		
	The Key Length should not be lower than 2048 or some platforms may con-	isider the certificate invalid.	c'est-a-dire : Common Name : inter
Digest Algorithm	sha256 🗸		calocal Country Code FR City
	The digest method used when the CA is signed		ea local, country coue int, city
	The best practice is to use SHA256 or higher. Some services and platforms	s, such as the GUI web server and OpenVPN, consider weaker digest	Strashourg Organization · COD loc
	algorithms invalid.		Strasbourg, Organization . COD.loc
Lifetime (days)	3650		Organizationnal Unit : IT
Common Name	internal-ca.cod.local		(2) Cliquer sur Save
	The following certificate authority subject components are optional and ma	ay be left blank.	
Country Code	FR 🗸		
State or Province	( A		
otate of Fronnee	Alsace		
City	Strasbourg		Une fois la CA enregistrée elle
Organization	COD.local		apparait dans la liste.
Organizational Unit	Л		• Issuer · self-signed $\rightarrow$ c'est u
			· · · · · · · · · · · · · · · · · · ·
	B Save 2		CA racine locale

- Certificates : 0  $\rightarrow$  aucun certificat encore généré avec cette CA.
- Valid From / Until : dates de validité.
- On pourra l'utiliser pour signer des certificats (VPN ou autre)

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN-CA	~	self-signed	0	ST=Alsace, OU=IT, O=COD.local, L=Strasbourg, CN=internal-ca.cod.local, C=FR Valid From: Sat, 19 Apr 2025 23:54:49 +0200 Valid Umit: Tue, 17 Apr 2035 23:54:49 +0200		<b>∅₩₽</b> €∎

Certificat créer

Cette section permet de consulter les certificats disponibles dans pfSense.

On y voit ici un certificat **auto-signé par défaut** utilisé pour l'accès HTTPS à l'interface d'administration (webConfigurator).

#### Ce qu'il faut savoir :

- Un certificat serveur signé par une CA est obligatoire pour sécuriser les connexions OpenVPN.
- Le certificat doit être de type "Server Certificate", afin d'être accepté par les clients OpenVPN.

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 37 / 197 - CHAHROUR Walid

Create / Edit CA				
Descriptive name	OpenVPN-CA           The name of this entry as displayed in the GUI for reference.           This name can contain spaces but it cannot contain any of the following characters: ?, <, 8, /, \`,'			
Method	Create an internal Certificate Authority			
Trust Store	<ul> <li>Add this Certificate Authority to the Operating System Trust Store</li> <li>When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.</li> </ul>			
Randomize Serial	Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.			



	_	ie revolation		
Search				Θ
Search term		Both	✓ Q Search	Clear
	Enter a searc	h string or *nix regular expression to search certificate names and distinguished name	s.	
Certificates				
Nome				
Name	Issuer	Distinguished Name	In Use	Actions
GUI default (68021b19c8228) Server Certificate CA: No Server: Yes	Issuer self-signed	Distinguished Name O=pfSense GUI default Self-Signed Certificate, CN=pfSense-68021b19c8228 Valid From: Fri, 18 Apr 2025 11:27:53 +0200 Valid Until: Thu, 21 May 2026 11:27:53 +0200	In Use webConfigurator	

Cliquer sur Add/Sign (bouton vert) pour créer un nouveau certificat signé Cette page permet de générer un certificat interne, signé par la CA créée précédemment.

Ce certificat est indispensable pour que le serveur OpenVPN puisse établir une connexion chiffrée avec les clients.

#### 🔅 Champs à renseigner :

• Method :

Laisser sur Create an internal Certificate  $\rightarrow$  on veut un certificat local, pas un certificat externe ou une demande de signature.

• Descriptive name :

Nom du certificat, visible uniquement dans pfSense (ex : OpenVPN-Server). Important pour différencier les certificats si plusieurs sont créés pour différents services.

	Add/Sign a New Certi	ficate	
Dans notre cas	Method	Create an internal Certificate	c'est
OpenVPN-Server	Descriptive name	OpenVPN-Server The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, 8, /,  `,`	

Ces informations sont intégrées dans le certificat et servent à identifier le serveur :

Champ	Description
Common Name	Nom du serveur (ex : vpn.cod.local) utilisé par OpenVPN. Doit correspondre à l'adresse utilisée par les clients.
Country Code	Code du pays (ex : FR).
State / City	Localisation (ex : Alsace / Strasbourg).
Organization / Unit	Nom du domaine ou de l'entreprise (ex : COD.local) et service (ex : IT).

**Remarque importante** : Le **Common Name** doit idéalement **correspondre au FQDN ou IP** utilisé par les clients VPN pour se connecter au serveur, afin d'éviter des erreurs de validation de certificat côté client.

→ Une fois ce formulaire rempli, il suffit de cliquer sur **Save** pour générer et signer le certificat. Il sera ensuite utilisable dans la configuration du serveur OpenVPN.



Internal Certificate		
Certificate authority	OpenVPN-CA 🗸	Dans notre cas nous
Key type	RSA	renseigner Common
	2048       The length to use when generating a new RSA key, in bits.       The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	Name : vpn.cod.local Country code DR
Digest Algorithm	sha256	
<u>Lifetime (days)</u>	3650 The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
Common Name	vpn.cod.local	
Country Code	The following certificate subject components are optional and may be left blank.           FR         •	
State or Province	Alsace	
City	Strasbourg	Catta agation normat
Organization	COD.local	d'ajouter des contrai
Organizational Unit	п	ou des informations

ction permet <sup>r</sup> des contraintes formations

#### supplémentaires au certificat. Détails des champs :

• Certificate Type :

Type d'utilisation du certificat.

- o Ici, il faut sélectionner Server Certificate (et non "User Certificate") si le certificat est destiné à un serveur OpenVPN.
- Un mauvais type peut empêcher le certificat d'être accepté pendant la connexion VPN.
- Alternative Names (SAN Subject Alternative Names) :

Permet d'ajouter d'autres noms ou adresses que le Common Name.

Par exemple : un FQDN, un nom DNS ou une IP utilisée par les clients pour joindre le serveur.

Ce champ est optionnel mais recommandé si plusieurs noms sont utilisés pour accéder au serveur (ex : vpn.cod.local, vpn.cod.lan, IP publique, etc.).

• Add SAN Row :

Bouton pour ajouter une ligne SAN.

#### Finalisation :

• Une fois tous les champs correctement remplis, cliquer sur Save pour générer et signer le certificat.



#### Cliquer sur Save

Certificate Attributes						
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.					
Certificate Type	User Certificate  Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.					
Alternative Names	FQDN or Hostname       Value         Type       Value         Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.					
Add SAN Row	+ Add SAN Row					
	a Save					

#### Problème détecté :

Dans la liste des certificats, le champ Certificate Type affiche :

- User Certificate
- Server : No

Cela signifie que le certificat a été généré en tant que certificat utilisateur, et non serveur.

#### Explication du problème :

Lors de l'étape précédente (capture 8), la valeur "Certificate Type" n'a pas été changée : elle est restée sur "User Certificate" au lieu de "Server Certificate".

Résultat : le certificat ne pourra **pas être utilisé pour un serveur OpenVPN**, car il n'est pas reconnu comme tel.

#### 🛠 Solution :

Tu dois recréer un nouveau certificat, en prenant bien soin de :

- Choisir le type Server Certificate,
- Conserver les mêmes paramètres (nom, Common Name, CA, etc.).

Une fois le bon certificat créé, tu verras dans la liste :

- Certificate Type : Server Certificate
- Server : Yes

#### Remarque :

Même si le certificat apparaît comme "User Certificate", il peut tout de même fonctionner pour OpenVPN.

Il est cependant recommandé de spécifier "Server Certificate" pour respecter les bonnes pratiques et garantir une compatibilité maximale avec tous les clients.





Created internal certificate Op	enVPN-Server	2			×
Authorities Certificates	Certificate	Revocation			
Search					<b>e</b>
Search term		Both	~	Q Search	Clear
	Enter a search	string or *nix regular expression to search certificate names and distinguished	names	i.	
Certificates					
Name	Issuer	Distinguished Name		In Use	Actions
GUI default (68021b19c8228) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-68021b19c8228 Valid From: Fri, 18 Apr 2025 11:27:53 +0200 Valid Umit: Thu, 21 May 2026 11:27:53 +0200	•	webConfigurator	<b>∥⇔₽</b> ∎C
OpenVPN-Server User Certificate CA: No	OpenVPN-CA	ST=Alsace, OU=IT, O=COD.local, L=Strasbourg, CN=vpn.cod.local, C=FR 🚯 Valid From: Sat, 19 Apr 2025 23:58:22 +0200 Valid Until: Tue, 17 Apr 2035 23:58:22 +0200			<b>∥*₽</b> ∎Ċ面
Server. NO					

#### En haut, on voit le message : "Created internal certificate OpenVPN-Server"

Cela confirme que la création du certificat s'est bien déroulée.

#### Création d'un utilisateur pour l'exportation du certificat

Cette capture montre le chemin pour accéder au

#### User Manager de pfSense.

#### em\_usermanager.php

	System -	(1) Cliquer sur System (2) Cliquer sur User Manager
	Advanced	
	Certificates	
1	General Setup	
əro	High Availability ,	
	Package Manager	
I	Register	
er	Routing	
>	Setup Wizard	
	Update	
	User Manager 2	
	Logout (admin)	

Cela permet de créer des comptes qui pourront ensuite être utilisés pour :

- L'authentification VPN,
- L'accès à l'interface d'administration (avec droits),
- D'autres services liés à l'utilisateur (certificat, portail captif, etc.).



#### Cas d'usage dans le cadre OpenVPN Road Warrior :

- Si tu ne relies pas encore pfSense à un annuaire (LDAP/Active Directory), tu peux :
  - o créer des utilisateurs locaux,
  - o et les utiliser pour s'authentifier au VPN.
- Ces utilisateurs peuvent également être associés à des **certificats** s'ils doivent utiliser une double authentification : **login + mot de passe + certificat**.



### dans pfSense, avec un certificat associé.

Ce type de compte est utilisé pour :

- Authentification VPN (mode *user auth + cert*)
- Tests internes sans dépendre d'un annuaire externe (Active Directory)

#### Détail des champs importants :

1. Username / Password : Identifiants que l'utilisateur saisira pour se connecter au VPN.

#### 2. Full name (facultatif) :

Sert uniquement à des fins administratives (nom descriptif dans l'interface).

#### 3. Certificate (✓) :

Cette case permet de générer **automatiquement un certificat utilisateur** lié à ce compte. Ce certificat sera nécessaire si l'authentification OpenVPN nécessite un **certificat client**, en plus du mot de passe.



User Properties		
Defined by	USER	
Disabled	This user cannot login	
Username	BTRINH	
Password		
2 Full name	Export User User's full name, for administrative information only	
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as I	MM/DD/YYYY
Custom Settings	<ul> <li>Use individual customized GUI options and dashboard layout for this user.</li> </ul>	
Group membership	admins	۵ ۲
	Not member of Mem	nber of
	>> Move to "Member of" list	Move to "Not member of" list
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	
3 Certificate	Click to create a user certificate	

Créer un **certificat numérique** associé à un compte utilisateur local. Ce certificat est utilisé pour établir une connexion VPN **authentifiée et chiffrée**, notamment dans un scénario OpenVPN avec authentification **par certificat client + mot de passe**.

#### Champ Description

**Descriptive name** Nom du certificat, visible dans l'interface pfSense (ex : vpn-user-export-cert).

Certificate Authority CA qui va signer le certificat (ici : OpenVPN-CA). Doit être valide et déjà créée.

Key Type / Length RSA 2048 bits – recommandé pour un bon équilibre sécurité/performance.

Digest Algorithm SHA256 – recommandé pour garantir l'intégrité de la signature.

Lifetime Durée de validité en jours (ex : 3650 = 10 ans).

Dans notre infrastructure, ce certificat est destiné à l'utilisateur BTRINH, afin qu'il puisse s'authentifier sur le serveur OpenVPN via :

• un login/mot de passe,





• et un certificat client personnel, qui sera exporté par la suite.

Create Certificate fo	r User	
Descriptive name	vpn-user-export-cert	Valider
Certificate authority	OpenVPN-CA v	
Key type	RSA	
	2048  The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
Digest Algorithm	sha256  The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
Lifetime	3650	
Keys		
Authorized SSH Keys	Enter authorized SSH keys for this user	
IPsec Pre-Shared Key		
Shell Behavior		
Keep Command History	□ Keep shell command history between login sessions If this user has shell access, this option preserves the last 1000 unique commands entered at a shell prompt between login sessions. The user an access history using the up and down arrows at an SSH or console shell prompt and search the history by typing a partial command and then using the up or down arrows.	

l'ensemble des paramètres de l'utilisateur local et **enregistrer le compte**, avec ou sans historique de commandes shell.

#### Keep Command History :

Cette option est utile uniquement si l'utilisateur accède au shell (via SSH ou console). Elle permet de **conserver un historique de 1000 commandes** entre les connexions. Dans la plupart des cas (comme ici, pour un usage VPN), cette option **n'est pas nécessaire**.

Cliquer sur Save		Shell Behavior				
		Keep Command History	C Keep shell command history between login sessions If this user has shell access, this option preserves the last 1000 unique commands entered at a shell prompt between login sessions. The user can access history using the up and down arrows at an SSH or console shell prompt and search the history by typing a partial command and then using the up or down arrows.			
Vérifier que l'utilisateur	e a bien été		Save			
ajouté à pf	Sense et qu'il e	st actif.				
Colonne	Description					
Username	Nom d'utilisat	eur, ici BTRIN	H			
Full Name	Description ad	ministrative v	visible, ici Export User			
Status	✓ indique que le compte est actif (non désactivé)					
Groups	Groupe(s) auquel appartient l'utilisateur (vide ici, ou admins pour le compte admin)					
Actions	🥕 Modifier le	e compte – 🔟	Supprimer			

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 44 / 197 - CHAHROUR Walid





#### Ce que cela confirme :

- Le compte est valide et activé.
- Le certificat (créé automatiquement) est associé.
- L'utilisateur est prêt pour l'**authentification VPN** si le serveur OpenVPN est configuré pour l'accepter.

Syste	System / User Manager / Users						
Users	Groups	Settings	Authentication Servers				
Users	lisername		Full name	Status	Groups	Actions	
	BTRINH		Export User	✓	Groups	in a cuons	
0	admin		System Administrator	~	admins	<b>A</b> <sup>0</sup>	





#### Configuration du VPN

Accéder au menu de gestion d'OpenVPN dans pfSense afin de :

- Créer un serveur VPN (mode Road Warrior),
- Gérer les clients, exportations, ou la topologie du tunnel,
- Suivre les connexions et journaux.
- (1) Cliquer sur VPN
- (2) Cliquer sur OpenVPN



Ce menu donne accès aux différents éléments de configuration :

- Servers : pour créer et configurer un serveur OpenVPN (notre objectif ici),
- Clients : (si pfSense doit se connecter à un VPN tiers),
- Client Export : pour générer les fichiers de configuration .ovpn,
- Wizard : assistant de configuration pas-à-pas.

Démarrer l'assistant de création d'un serveur OpenVPN.

Cet assistant guide étape par étape la configuration :

- du certificat serveur,
- de la méthode d'authentification (utilisateur, LDAP...),
- du réseau VPN (adresse, routage...),
- du chiffrement et des options de sécurité.

VPN / OpenVPN / Servers				Lii 🗉 😧	
Servers	Clients Client Specific Overrides	Wizards Client Export			
OpenVPN	N Servers				
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
					+ Add

L'assistant OpenVPN commence par demander le **type de backend d'authentification** à utiliser pour les connexions VPN.

Cette option détermine comment les utilisateurs seront **authentifiés** lors de la tentative de connexion.

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 46 / 197 - CHAHROUR Walid





#### Type of Server :

Ce menu déroulant permet de sélectionner la méthode d'authentification parmi :

- Local User Access (comptes internes pfSense),
- LDAP (Active Directory ou autre annuaire compatible),
- RADIUS (serveur d'authentification réseau),
- etc.

OpenVPN Remote Access Server Setup					
	This wizard will provide guidance through an OpenVPN Remote Access Server Setup .				
	The wizard may be stopped at any time by clicking the logo image at the top of the screen.				
Select an Authenticat	tion Backend Type				
Type of Server	LDAP 🗸 1				
	NOTE: If unsure, leave this set to "Local User Access."				
	» Next 2				

Ici, le **type LDAP** est sélectionné, car l'authentification sera **déléguée à un Active Directory** configuré en amont dans pfSense.

Cela permet d'intégrer la solution VPN à l'environnement **de gestion centralisée des identités** de l'organisation.

#### Intérêt d'une authentification LDAP :

- Permet l'utilisation des comptes utilisateurs déjà existants dans l'entreprise.
- Évite la duplication des identifiants.
- Renforce la sécurité en unifiant les règles de mot de passe et de politique d'accès.

Configurer la connexion entre pfSense et le **serveur LDAP (Active Directory)**, afin que ce dernier soit utilisé comme **backend d'authentification** pour les utilisateurs VPN.

#### Champ Description

Name Nom administratif de la connexion LDAP (ex. OpenVPN-CA). N'a aucun impact sur le fonctionnement, il sert uniquement à l'identification dans pfSense.

Hostname or IPAdresse du serveur Active Directory. Dans ce cas : 192.168.10.10. Ce champ peutaddresscontenir un FQDN si la résolution DNS est fonctionnelle.

Port utilisé pour le protocole LDAP. Le port 389 est le port standard pour une connexion LDAP non chiffrée (TCP simple).

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 47 / 197 - CHAHROUR Walid



dans

## BTSSID

hamp	Description
Transport	Définit si la communication avec l'AD se fait en clair (Standard TCP) ou via une connexion sécurisée (STARTTLS, SSL/TLS).
Protocol Version	Version LDAP utilisée, généralement 3.
Search Scope Level	Détermine si la recherche s'effectue uniquement dans un conteneur spécifique ou tout l'annuaire (ici Entire Subtree).

LDAP Authentication	Server Parameters		
Name	OpenVPN-CA		
	Descriptive server name, for administrative reference.		
Hostname or IP address	192.168.10.10		
	Address of the LDAP server. When using SSL/TLS or STARTTLS, this hostname r	must match the LDAP server certificate.	
Port	389		
	LDAP Server port, leave blank for the default (389 for TCP or STARTTLS, 636 for	SSL/TLS).	
Transport	Standard TCP		
	The transport used by the LDAP server. It can either be standard TCP, STARTTLS	or SSL/TLS Encrypted.	
Peer Certificate Authority	global 🗸		
	The Certificate Authority for the LDAP server certificate. Used for SSL/TLS and S	STARTTLS.	
Protocol Version	3 🗸		
Server Timeout	25		Le bon fonctionnement de
Search Scone Level	Entire Subtree		cette étane dépend ·
Search Scope Base DN	DC=COD,DC=local		• D'une connectivite
Authentication	OU=VPNUsers,DC=COD,DC=local	6	réseau fonctionnelle entre
Containers	Semi-Colon separated. This will be prepended to the search base dn above or ful EXAMPLE: CN-Users;DC=example	Il container path can be specified.	pfSense et le serveur AD,
	EXAMPLE: CN=Users,UC=example,UC=COM;OU=OtherUsers,DC=example,DC=CO	m	

- D'une configuration correcte du bind DN (à venir dans l'étape suivante),
- D'un horodatage synchronisé entre les deux machines (important avec TLS).

Définir les paramètres d'identification utilisés par pfSense pour :

- 1. Se connecter au serveur LDAP (via un compte de service),
- 2. Rechercher et authentifier les utilisateurs.

Champ	Description
LDAP Bind User DN	Identifiant utilisé pour interroger l'annuaire. Ici : btrinh@COD.local, compte de service disposant des droits nécessaires à la lecture LDAP.
LDAP Bind Password	Mot de passe du compte ci- dessus. Il ne s'agit pas d'un compte utilisateur VPN, mais d'un compte technique servant uniquement aux requêtes LDAP.





#### Champ

Description

Attributs	d'identification	
Champ	Valeur	Rôle
		C'00

User Naming Attribute	sAMAccountName	correspondant au nom d'utilisateur Windows (ex. : btrinh).	
Group		Permet de retrouver les	
Naming	sAMAccountName groupes via leur nom		

Attribute NetBIOS/Windows stand

Cliquer sur **Add new Server** permet d'enregistrer le connecteur LDAP dans pfSense. Il pourra ensuite être sélectionné comme **méthode d'authentification** lors de la configuration du serveur OpenVPN.

Ces attributs sont compatibles avec Microsoft Active Directory.

Extended Query	
	Example: memberOf=CN=Groupname,OU=MyGroups,DC=example,DC=com
LDAP Bind User DN	btrinh@COD.local
	If left blank, an anonymous bind will be done.
LDAP Bind Password	
	If a user DN was supplied above, this password will also be used when performing a bind operation.
User Naming Attribute	sAMaccountName
, , , , , , , , , , , , , , , , , , ,	Typically "cn" (OpenLDAP, Novell eDirectory), "samAccountName" (Microsoft AD)
Group Naming Attribute	cAMAccountblopp
oroup running Autobate	Typically "cn" (OpenLDAP, Microsoft AD, and Novell eDirectory)
Member Naming	member
Attribute	Typically "member" (OpenLDAP), "memberOf" (Microsoft AD), "uniqueMember" (Novell eDirectory)
RFC 2307 Groups	LDAP Server uses RFC 2307 style group membership.
	RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active
	Directory style group membership (R+C 2307bis).
Group Object Class	posixGroup
	Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".
UTF8 Encode	UTF8 encode LDAP parameters before sending them to the server.
	Required to support international characters, but may not be supported by every LDAP server.
Username Alterations	□ Do not strip away parts of the username after the @ symbol.
	e.g. user@host becomes user when unchecked.
Allow unauthenticated	Allow unauthenticated bind
bind	<ul> <li>Unauthenticated binds are bind with an existing login but with an empty password.</li> </ul>
	3) Add new Server 4

#### Option Description

UTF8Permet d'encoder les requêtes LDAP en UTF-8. À activer pour gérer correctement lesEncodecaractères accentués ou spéciaux.

Associer un certificat SSL/TLS valide au service OpenVPN.

Ce certificat est utilisé pour authentifier le serveur auprès des clients et établir une connexion chiffrée.

#### Champ Description

**Certificate** Sélection du certificat précédemment généré dans pfSense. Ici, le certificat OpenVPN-Server est choisi. Il a été signé par la CA interne OpenVPN-CA.

Le certificat permet :

- de garantir l'identité du serveur VPN (évite les attaques de type "man-in-the-middle"),
- d'initier une communication sécurisée avec les clients VPN via le protocole TLS.

Le certificat doit impérativement :

• être de type Server Certificate,

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 49 / 197 - CHAHROUR



• être signé par une CA de confiance (en l'occurrence, la CA interne créée au début du projet).

Server Certificate Selection	Cliquer sur <b>Next</b>	
OpenVPN Remote Access Server Setup Wizard	pour poursuivre	
Choose a Server Certificate	l'assistant at passor	
Certificate OpenVPN-Server	à la configuration	
>> Add new Certificate >> Next	réseau du tunnel	
	VPN.	

Associer au serveur OpenVPN une **autorité de certification (CA)** de confiance, qui a servi ou servira à **signer les certificats client**.

#### Champ Description

Certificate<br/>AuthoritySélection de la CA interne utilisée dans la configuration. Ici : OpenVPN-CA, créée au<br/>début du projet. Elle signe les certificats serveur et client utilisés dans la communication<br/>VPN.

#### Rôle de la CA :

- Elle permet à pfSense (serveur VPN) de vérifier que les certificats clients présentés sont valides,
- Elle est **indispensable dans une architecture basée sur TLS** où l'authentification par certificat est active.

#### Pré-requis :

Avant d'arriver à cette étape, il est impératif d'avoir :

- Créé une CA interne (ou importé une CA externe),
- Utilisé cette CA pour signer le certificat serveur (et éventuellement les certificats utilisateurs).

Cliquer sur <b>Next</b> pour	Certificate Authority	Selection		
poursuivre l'assistant		OpenVPN Remote Access Server Setup Wizard		
de configuration	Choose a Certificate	Authority (CA)		
OpenVPN, qui	Certificate Authority	OpenVPN-CA	~	
enchaînera sur les		>> Add new CA >> Next		
parametres reseau du				
tunnel.				



Définir l'identifiant administratif du serveur VPN et les **paramètres d'écoute réseau** sur pfSense. Cela permet de préciser comment le serveur va accepter les connexions des clients. **Détail des champs :** 

#### Description

- Nom donné au serveur OpenVPN (ex. : OpenVPN Road Warrior).
- Utilisé à titre administratif pour identifier ce service dans pfSense.
- Il est également affiché dans les fichiers générés par le module **OpenVPN Client Export**, facilitant la reconnaissance du profil VPN côté client.

#### Protocol

- Choix entre **UDP** ou **TCP** pour les connexions VPN.
- Ici : UDP on IPv4 only, recommandé pour les performances (moins de surcharge que TCP).
- • Interface
- Interface réseau sur laquelle pfSense écoutera les connexions VPN entrantes.
- Généralement WAN, sauf dans des cas spécifiques (VPN interne, site à site, etc.).

#### Local Port

- Port d'écoute du serveur OpenVPN.
- Par défaut : 1194, le port standard du protocole OpenVPN.
- Peut être modifié si un autre service utilise déjà ce port, ou pour des raisons de sécurité (obscurcissement).

Server Setup		
	OpenVPN Remote Access Server Setup Wizard	
General OpenVPN Ser	temote Access Server Setup Wizard  ation  Road Warrior this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the . "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.  v4 only use for OpenVPN connections. If unsure, leave this set to UDP.  e where OpenVPN will listen for incoming connections (typically WAN.)	
Description	OpenVPN Road Warrior A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.	
Endpoint Configuratio	on	
Protocol	UDP on IPv4 only	
Interface	WAN   The interface where OpenVPN will listen for incoming connections (typically WAN.)	
Local Port	1194 Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.	

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 51 / 197 - CHAHROUR Walid





Définir les **algorithmes de chiffrement et d'authentification TLS** utilisés par le serveur OpenVPN afin de garantir :

- l'intégrité des communications,
- la confidentialité des données,
- la vérification mutuelle de l'identité des participants.

#### Paramètre Description

**Protocol** UDP on IPv4 only – recommandé pour ses performances.

Interface WAN – interface réseau d'écoute pour les connexions VPN.

Local Port 1194 – port standard d'OpenVPN, personnalisable si nécessaire.

#### Cryptographic Settings :

Paramètre	Description
TLS Authentication	Coche activée $\rightarrow$ active une couche supplémentaire de sécurité en exigeant une <b>clé</b> <b>TLS pré-partagée</b> pour l'authentification du canal TLS. Cela empêche les connexions non autorisées (DoS, scans réseau, etc.).
Generate TLS Key	Permet à pfSense de <b>générer automatiquement</b> cette clé TLS.
DH Parameters Length	2048 bits – Longueur des paramètres Diffie-Hellman pour l'échange de clé sécurisé. Valeur recommandée en entreprise (équilibre entre sécurité et performance).

#### Data Encryption Algorithms :

Ce champ permet de sélectionner les **algorithmes de chiffrement symétrique** négociés avec les clients. Dans cette configuration, trois algorithmes sont proposés :

- **AES-256-GCM** : très sécurisé, recommandé par la plupart des standards actuels.
- AES-128-GCM : plus rapide, mais légèrement moins sécurisé.
- CHACHA20-POLY1305 : performant sur CPU sans accélération matérielle AES.

**Bonne pratique** : Laisser les trois algorithmes listés dans cet ordre permet aux clients de négocier le plus fort qu'ils supportent.

Activer TLS Authentication est fortement recommandé pour la sécurité.

AES-256-GCM est généralement préféré sauf contraintes matérielles.

La longueur de clé Diffie-Hellman doit être au minimum de 2048 bits pour respecter les politiques de sécurité d'entreprise.



Endpoint Configurati	on	
Protocol	UDP on IPv4 only	
	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.	
Interface	WAN	
	The interface where OpenVPN will listen for incoming connections (typically WAN.)	
Local Port	1194	
	Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.	
Cryptographic Settin	gs	l
TLS Authentication	Enable authentication of TLS packets.	
Generate TLS Key	Automatically generate a shared TLS authentication key.	
TLS Shared Key		Configurer les
	Paste in a shared TLS key if one has already been generated.	
DH Parameters Length	2048 bit ~	
	Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.	
Data Encryption Algorithms	AES-256-GCM AES-128-GCM CHACHA20-POLY1305	
	List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.	

algorithmes de secours, le hachage d'authentification des paquets VPN, et les ressources matérielles utilisées pour accélérer le chiffrement.

#### Détail des paramètres :

Paramètre	Description
Fallback Data Encryption Algorithm	AES-256-CBC : algorithme utilisé <b>en secours</b> si la négociation principale échoue. Il offre un chiffrement fort basé sur un bloc de 128 bits avec une clé de 256 bits. Cela garantit que la communication reste chiffrée même dans des conditions de compatibilité dégradée.
Auth Digest Algorithm	SHA256 (256-bit) : algorithme de hachage utilisé pour l' <b>authentification des messages</b> <b>TLS</b> . Il permet de vérifier que les données transmises n'ont pas été altérées. Ce paramètre doit être le <b>même côté client et serveur</b> .
Hardware Crypto	No Hardware Crypto Acceleration : désactive l'utilisation d'un <b>accélérateur</b> <b>cryptographique matériel</b> . Ce choix est adapté si le matériel ne dispose pas d'un moteur de chiffrement compatible (comme AES-NI sur les processeurs Intel). Sur un serveur de production, l'activation peut améliorer les performances.



## BTSSIO

Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block)
	The algorithm used to encrypt traffic between endpoints when data encryption negotiation is diabled or fails.
Auth Digest Algorithm	SHA256 (256-bit) 🗸
	The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto	No Hardware Crypto Acceleration
	The hardware cryptographic accelerator to use for this VPN connection, if any.

Définir la topologie réseau du VPN, c'est-à-dire :

- le réseau attribué aux clients VPN (Tunnel Network), •
- le réseau local à atteindre via le tunnel (Local Network), ٠
- les limitations de connexion et les options de sécurité complémentaires. ٠

#### Pv4 Tunnel Network

Valeur: 10.8.0.0/24

#### Ce champ définit le réseau IP virtuel utilisé pour les connexions VPN.

- La première adresse (ex. 10.8.0.1) sera assignée au serveur VPN. ٠
- Les adresses suivantes seront distribuées aux clients VPN.
- Ce réseau ne doit pas être en conflit avec le LAN ou d'autres sous-réseaux déjà en place. ٠

#### IPv4 Local Network

Valeur : 192.168.10.0/24

Il s'agit du réseau interne (LAN) que les clients VPN pourront atteindre une fois connectés.

- Cela permet aux clients d'accéder aux ressources internes de l'entreprise (serveurs, imprimantes, NAS, etc.).
- Cette route est automatiquement poussée vers les clients lors de l'établissement du tunnel. ٠

#### **Concurrent Connections**

Valeur: 10

Définit le **nombre maximum de clients** autorisés à se connecter simultanément à ce serveur OpenVPN.

Cette limitation peut être adaptée en fonction des besoins et des capacités de l'infrastructure. •



• Elle est utile pour contrôler l'accès ou prévenir la surcharge.



Une fois ces paramètres définis, l'assistant poursuivra avec la configuration des

options DNS/DHCP poussées aux clients.

Définir les paramètres de **résolution de noms (DNS)**, **synchronisation horaire (NTP)** et éventuellement **NetBIOS**, transmis aux clients VPN lors de leur connexion.

#### Détail des champs principaux :

#### DNS Default Domain

Valeur : COD.lan

BTSSID

- Ce champ permet d'attribuer un suffixe DNS par défaut aux clients.
- Cela facilite la résolution de noms internes : un client pourra par exemple pinguer serveur1 au lieu de serveur1.COD.lan.

#### NS Server 1 & DNS Server 2

Valeurs : 192.168.10.10 et 192.168.10.30

- Ces adresses pointent généralement vers les **contrôleurs de domaine Active Directory** disposant du rôle **DNS**.
- Elles permettent aux clients VPN de :
  - o résoudre les noms internes (ordinateurs, serveurs, imprimantes),
  - joindre les ressources internes comme s'ils étaient physiquement présents sur le réseau local.



lient Settings		
Dynamic IP	Allow connected clients to retain their connections if their IP address changes.	
Topology	Subnet – One IP address per client in a common subnet Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (IOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".	
dvanced Client Sett	ings	
DNS Default Domain	COD.lan Provide a default domain name to clients.	
DNS Server 1	192.168.10.10       DNS server IP to provide to connecting clients.	
DNS Server 2	192.168.10.30 DNS server IP to provide to connecting clients.	
DNS Server 3	DNS server IP to provide to connecting clients.	
DNS Server 4	DNS server IP to provide to connecting clients.	
NTP Server	Network Time Protocol server to provide to connecting clients.	Ces paramè assurent au
NTP Server 2	Network Time Protocol server to provide to connecting clients.	clients VPN <b>expérience</b>
NetBIOS Options	Enable NetBIOS over TCP/IP.  If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.	réseau
NetBIOS Node Type	none	

**poste local**, avec accès direct aux ressources internes grâce à la résolution DNS et au routage configuré précédemment.

Créer les règles de pare-feu indispensables pour :

- -Permettre l'établissement de la connexion VPN depuis Internet,
- Autoriser le trafic interne des clients à travers le tunnel VPN.
- Firewall Rule Traffic from clients to server
- Coche activée
- Ajoute une règle sur l'interface **WAN** autorisant l'accès au **port du serveur OpenVPN** (par défaut : UDP 1194).
- Sans cette règle, aucun client ne pourra initier de connexion VPN depuis l'extérieur.

#### OpenVPN Rule – Traffic from clients through VPN

- Coche activée 🗹
- Ajoute une règle sur l'interface **OpenVPN** autorisant **tout le trafic sortant** des clients VPN vers le réseau local.
- Sans cette règle, les clients VPN pourront se connecter au serveur, mais **ne pourront pas accéder aux ressources internes** (réseau, DNS, fichiers, etc.).

#### Remarques importantes :

• Ces règles peuvent être **modifiées manuellement** après l'assistant pour affiner la sécurité (ex. : filtrer certains protocoles ou IP).



• Il est essentiel de limiter les accès dans un environnement de production (principe du moindre privilège).

		Cliquer							
Firewall Rule Config	uration	sur <b>Next</b>							
	OpenVPN Remote Access Server Firewall Rules								
	Rules control passing or blocking network traffic as it flows through the firewall.								
	Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.	terminer							
	The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.	la							
Traffic from clients	to server								
Firewall Rule	Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.								
Traffic from clients	through VPN 1								
OpenVPN rule	Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.								
	>> Next 2								

configuration du serveur VPN, avec les règles de pare-feu ajoutées automatiquement.

Afficher un message de confirmation indiquant que **le serveur OpenVPN est maintenant opérationnel**, et rappeler les prochaines actions possibles (ajout d'utilisateurs, export des clients, etc.). **Résultat de la configuration :** 

- Le serveur VPN est actif sur l'interface WAN, prêt à recevoir des connexions.
- Les **règles de pare-feu** ont été générées automatiquement pour autoriser le trafic entrant et sortant.
- Les certificats (serveur et utilisateurs) sont correctement liés à la CA interne.
- La méthode d'authentification LDAP permet de sécuriser les accès en s'appuyant sur un Active Directory déjà en place.



Cliquer sur Finis pour passer à la prochaine étape





Afficher un **récapitulatif technique** de l'instance OpenVPN active. Cette vue permet de contrôler les paramètres essentiels du serveur VPN et d'accéder aux fonctions de gestion (édition, duplication, suppression).

Servers	Clients C	lient Specific Overrides	Wizards		
OpenVPN	N Servers				
Interface	Protocol / Por	t Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.8.0.0/24	Mode: Remote Access ( User Auth ) Data Ciphers: AES-256-GCM, AES-128-GCM, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN Road Warrior	<b>₽</b> □ <b></b>
					+ Ad

Cette vue confirme que le **serveur OpenVPN est actif, sécurisé et prêt à être utilisé** par des utilisateurs distants. Il constitue désormais un **point d'entrée sécurisé** au réseau interne de l'organisation, tout en s'intégrant à l'infrastructure Active Directory existante via LDAP.

### **Installation module exportation du client VPN**

Accéder au **Package Manager** de pfSense afin d'installer un **module tiers** : openvpn-client-export. Ce package facilite considérablement la génération des profils. ovpn nécessaires à la connexion des clients VPN.

#### Fonction du Package Manager :

Le gestionnaire de paquets de pfSense permet :

- D'installer des extensions officielles pour étendre les fonctionnalités,
- De maintenir ces packages à jour,
- De désinstaller ceux devenus inutiles.





	oo noo genyny	ŀ
	System -	۲ ۲
	Advanced	t
	Certificates	
	General Setup	
	High Availability	
	Package Manage	
	Register	
	Routing	
	Setup Wizard	
	Update	
	User Manager	
	Logout (admin)	
-	•	

Accéder à l'onglet **Available Packages**, rechercher **openvpn-client-export**, puis procéder à son installation. Tu peux m'envoyer cette prochaine capture, et je continuerai dans le même ton technique et structuré.

Rechercher et installer le **module d'exportation des clients OpenVPN** depuis le gestionnaire de paquets de pfSense. Ce module permet de :

- Générer facilement les fichiers de configuration .ovpn,
- Créer des installeurs Windows auto-configurés,
- Exporter des profils adaptés aux systèmes Windows, macOS, Linux, Android et iOS.

#### **Onglet**: Available Packages

Accès à tous les packages installables depuis pfSense.

- (1) **Onglet** : Available Packages Accès à tous les packages installables depuis pfSense.
- (2) **Recherche** : "VPN" Permet de filtrer les paquets liés aux technologies VPN. Ici, on cible **openvpn-client-export**.
- (3) Package identifié :
- Nom : openvpn-client-export
- Version : 1.9.2 (dans cet exemple)



## BTSSIO

module :

•

- Description : "Exports pre-configured OpenVPN Client configurations directly from pfSense software."
- Cliquez sur **Install** pour lancer l'installation.



- de fichiers .ovpn prêts à l'emploi,
- Création d'exécutables pour installation rapide sur Windows (.exe), .
- Inclusion des certificats, options de chiffrement et serveurs DNS,
- Options de personnalisation (authentification, interface, compression...). .

Valider l'installation du package d'exportation de clients VPN. Cette confirmation déclenche le téléchargement et l'installation automatique du package et de ses dépendances.

Cliquer sur le bouton Confirm permet à pfSense de :

- télécharger le package depuis ses dépôts officiels, •
- vérifier son intégrité, •
- l'intégrer à l'interface Web. •



Afficher l'état d'avancement du téléchargement et de l'installation des composants nécessaires au bon fonctionnement du module d'export.

Les paquets suivants sont installés :

- **openvpn-client-export** (version 1.9.2) : cœur du module d'exportation. •
- 7-zip : utilisé pour compresser certains fichiers d'installation.

Epreuve E6 – Situation professionnelle 2 - Documentation Technique - Page 60 / 197 - CHAHROUR





• zip, libsysinfo, openvpn-client-export-2.6.7 : dépendances internes.

Le message indique :

- 5 paquets à installer,
- 31 MiB d'espace requis,
- L'opération est en cours (étape 1 sur 5).



Le package est désormais opérationnel, comme l'indique le message :

System / Package Manager / Package Installer	0
pfSense-pkg-openvpn-client-export installation successfully completed.	
Installed Packages Available Packages Package Installer	
Package Installation	
[4/5] Installing 7-zip-23.01	
[4/5] Extracting 7-21-23.01: done	
[5/5] Fistalling preense-pkg-openvpn-client-export-1.9.2	
[J/J] Excludeding probability of the second se	
done.	
Loading package configuration done.	
Configuring package components	
Loading package instructions	
Custom commands	
Executing custom_php_install_command()done.	
Writing configuration done.	
>>> Cleaning up cache done.	U
Success	•
	1

### Vérification règles Firewall

Afficher, modifier ou ajouter des règles de filtrage réseau dans pfSense, pour :

- Autoriser le trafic VPN entrant (depuis WAN),
- Contrôler le trafic entre les clients VPN et les ressources internes,



• Appliquer des **restrictions de sécurité supplémentaires** (ex. : bloquer certains ports, limiter à certaines IP...).

Même si l'assistant OpenVPN peut les créer automatiquement, une revue manuelle permet de :

- Affiner les droits d'accès des utilisateurs VPN,
- Appliquer le principe du moindre privilège,
- Garantir une **conformité** avec la politique de sécurité de l'entreprise.

System <del>-</del>	Interfaces 🕶	Firewall 🗕	Sentces -
		Aliases	
enVPN/S	ervers	NAT	
		Rules	2
Clients Clier	nt Specific Overrid	Schedules	
		Traffic Shape	r
ervers		Virtual IPs	
rotocol / Port	Tunnel Network	Mode / C	rypto

Sans cette autorisation, **aucun client externe** ne pourra initier de connexion VPN.

Le port 1194 en UDP est celui par défaut d'OpenVPN, mais peut être modifié en fonction de la configuration.

Fl	oatin	g V	VAN L	AN E	MZ	OpenVPN						
Ru	ıles	(Drag 1	to Chang	e Order)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	0/0 B	IPv4 *	*	*	*	*	*	none			₺₡₽©₫×
þ	~	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN OpenVPN_RW_AD wizard	ᢤ∥̂⊡⊘≣́×
-									Ĵ	Add 🕽 Ad	dd 🛅 Delete 🚫 Toggle [ Copy	🕞 Save 🕂 Separato

Permettre aux **utilisateurs connectés via le VPN** d'émettre du trafic vers le réseau interne. Cette règle est indispensable pour **autoriser le transit des paquets** à l'intérieur du tunnel VPN.

Flo	ating	WA	N LAN	I DM	z	OpenVPN							
Ru	les (	Drag to States	Change ( Protocol	Order) Source	Port	Destination	Port	Gateway	Queue	Schedule	Description		Actions
	~	0/0 B	IPv4*	*	*	*	*	*	none		OpenVPN OpenVPN_RW_A	D wizard	ᢤᢞ᠋ᢩ᠐᠐ᢆ᠋ <u>ᡝ</u> ᢂ
	_				_		_			1 Add	🕽 Add 🛅 Delete 🚫 1	Toggle 🚺 Copy	Save + Separator

#### i

- Cette règle permet aux clients VPN d'accéder aux ressources du réseau local (ex. : serveurs AD, partages, messagerie...).
- Elle autorise **tout le trafic sortant**, ce qui est pratique en environnement de test ou lors d'une configuration initiale.



### **Configuration du client de l'exportation**

Accéder à toutes les fonctionnalités liées à OpenVPN dans pfSense, notamment :

- La gestion des serveurs VPN,
- La configuration des clients (client-to-site),
- Les exports via l'onglet Client Export (visible après installation du package).



Définir les options de connexion que le fichier .ovpn ou l'installeur OpenVPN utilisera lors du **déploiement sur les postes clients**.

Option	Description
Remote Access Server	Sélection du serveur OpenVPN à utiliser (ici OpenVPN_RW_AD UDP4:1194).
Host Name Resolution	Permet de spécifier l'adresse publique ou IP locale utilisée par les clients pour se connecter.
Host Name	Dans notre cas : 192.168.1.254 – c'est l'IP publique (ou IP NATée) du pare-feu <b>vue</b> depuis l'extérieur.
Verify Server CN	Vérifie le nom commun (CN) du certificat serveur – utile pour sécuriser la connexion.
Silent Installer	Génère un exécutable Windows prêt à installer sans intervention de l'utilisateur.
Block Outside DNS	Empêche les fuites DNS en forçant l'usage des DNS internes VPN.
Bind Mode	Contrôle si le client doit lier le port local (optionnel).



OpenVPN Server							
Remote Access Server	OpenVPN_RW_AD UDP4:1194 V						
Client Connection Be	havior						
Host Name Resolution	Other 🗸 🔰						
Host Name	192.168.1.254       Enter the hostname or IP address the client will use to connect to this server						
Verify Server CN	Automatic - Use verify-x509-name where possible						
Block Outside DNS Discrete across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option not affected.							
Legacy Client	Legacy Client Do not include OpenVPN 2.5 and later settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.						
Silent Installer	Create Windows installer for unattended deploy. Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.						
Bind Mode	Do not bind to the local port						

Définir les **paramètres de stockage, chiffrement et sécurité** des certificats et profils VPN à destination des utilisateurs finaux.

#### **Option Fonction**

PKCS#11 Certificate Storage	Permet l'usage de <b>tokens matériels</b> (HSM, cartes à puce) pour sécuriser le certificat client.
Microsoft Certificate Storage	Stocke le certificat dans le <b>magasin de certificats Windows</b> , utile pour l'intégration système.
Password Protect Certificate	Protège le certificat PKCS#12 avec un mot de passe. Recommandé pour les profils sensibles.
PKCS#12 Encryption Nive	au de chiffrement pour le bundle client (ex. : AES-256 + SHA256, recommandé)
Use a Proxy Active l'usage	e d'un <b>proxy réseau</b> pour les clients OpenVPN.
Additional configuration	Ajoute des options personnalisées au fichier .ovpn (ex. : remote-random,

Additional configurationAjoute des options personnalisées au fichier .ovpn (ex. : remote-randomoptionsroute-delay, etc.).

Save as default Enregistre ces paramètres comme configuration par défaut pour tous les exports futurs.



Certificate Export Op	itions
PKCS#11 Certificate Storage	Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
Microsoft Certificate Storage	Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate	Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.
PKCS#12 Encryption	High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windo 🔹 Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program
Proxy Options	
Use A Proxy	Use proxy to communicate with the OpenVPN server.
Advanced	
Additional configuration options	
	Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
	EXAMPLE: remote-random;
	Save as default

Cliquer sur Save as default

BTSSID

### **Exportation du client OPenVPN**

Ouvrir le panneau de gestion OpenVPN dans pfSense pour :

- Vérifier l'état du serveur VPN,
- Accéder à l'onglet Client Export,
- Télécharger les profils VPN générés automatiquement pour chaque utilisateur ayant un certificat valide.



L'onglet **Client Export** est désormais visible grâce à l'installation du package openvpn-client-export.

Il permet de générer :

- Un fichier .ovpn (configuration brute),
- o Un .exe (installeur Windows auto-configuré),
- Une archive .zip (certificat + clé + profil),

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 65 / 197 - CHAHROUR Walid





 Des profils compatibles OpenVPN Connect, Viscosity, Tunnelblick ou encore Linux NetworkManager.

VPN / OpenVPN / Servers							
Servers	Clients Client	: Specific Overrides	Wizards Client Export				
OpenVPN Servers nterface Protocol / Port Tunnel Network Mode / Crypto Description Action:							
WAN	UDP4 / 1194 (TUN)	10.8.0.0/24	Mode: Remote Access ( User Auth ) Data Ciphers: AES-256-GCM, AES-128-GCM, AES-256-CBC Digest: SHA256	OpenVPN Road Warrior	∥0亩		

#### Cliquer sur Client Export

Permettre aux utilisateurs de **télécharger leur configuration OpenVPN prête à l'emploi**, selon leur système d'exploitation et méthode de déploiement.

#### **Inline Configurations**

Ces formats embarquent tous les éléments (certificat, clé, paramètres) dans un seul fichier .ovpn.

- Most Clients : Fichier .ovpn standard pour Windows/Linux/Mac.
- Android : Adapté aux applications mobiles comme OpenVPN for Android.
- OpenVPN Connect (iOS/Android) : Compatible avec l'application officielle **OpenVPN Connect**.

#### **Bundled Configurations**

Ces options séparent ou regroupent les fichiers nécessaires :

- Archive (.zip) : Contient le .ovpn, les certificats, les clés.
- Config File Only : Le fichier .ovpn seul, sans certificat séparé.

#### Windows Installer

- 64-bit / 32-bit : Installeur Windows préconfiguré pour l'utilisateur (inclut tous les éléments dans un .exe autonome).
- L'utilisateur peut choisir le format de configuration le plus adapté.
- L'administrateur peut fournir un fichier sécurisé et immédiatement fonctionnel.



# BTSSIO

	Select the level of encryption to use when exporting a PK	CS#12 archive. Encryption support varies by Operating System and program	
Proxy Options			
Use A Proxy	□ Use proxy to communicate with the OpenVPN server.		
Advanced			
Additional configuration options	Enter any additional options to add to the OpenVPN client	t export configuration here, separated by a line break or semicolon.	
	EXAMPLE: remote-random;		
	Save as default		0
Search		•	
Search term		Q Search 💆 Clear	
	Enter a search string or *nix regular expression to search	h.	
OpenVPN Clients			
User	Certificate Name	Export	
Authentication Only (No Cert	none	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Current Windows Installer (2.6.7-tx001): 64-bit 32-bit	•

#### Cliquer sur Most client pour exporter la configuration

Ce fichier .ovpn contient tous les paramètres nécessaires à la connexion VPN via un client OpenVPN (Windows, Linux, macOS, Android, iOS...).



joindre un hôte du réseau le tunnel VPN, mais la

échoue avec le message suivant :

Délai d'attente de la demande dépassé.

Cela s'explique de manière logique et attendue par le fait que la configuration OpenVPN n'est pas encore finalisée et que le client distant n'est pas encore connecté au réseau VPN, ni intégré au sous-réseau local géré par le routeur pfSense.

À ce stade de la mise en place, il est normal que le client distant ne puisse pas accéder aux ressources internes (comme le serveur Active Directory). La connectivité réseau ne sera possible qu'une fois la configuration du serveur OpenVPN activée, que le client se connecte correctement au service VPN, et que les règles de pare-feu ainsi que les routes réseau soient appliquées.







#### Étape préalable : téléchargement et installation du client

Avant d'accéder à cette interface, il est nécessaire de **télécharger et installer le client officiel OpenVPN Connect** sur le poste utilisateur. Ce logiciel permet d'importer un fichier de configuration et d'établir une connexion VPN vers un serveur distant.

#### Lien de téléchargement officiel :

https://openvpn.net/client-connect-vpn-for-windows/

#### Procédure d'installation :

- 1. Accéder au lien ci-dessus à l'aide d'un navigateur Internet.
- 2. Télécharger la version du client correspondant au système d'exploitation utilisé.
- 3. Lancer le fichier exécutable (.exe) téléchargé.
- 4. Suivre l'assistant d'installation par défaut jusqu'à la fin.

#### Interface de connexion - Premier lancement

Une fois le client OpenVPN Connect installé et lancé, l'interface ci-dessus s'affiche. Elle propose deux méthodes de connexion :

- URL : saisie manuelle de l'adresse d'un serveur ou d'un ID cloud (non utilisée dans notre cas),
- UPLOAD FILE : importation d'un fichier de configuration .ovpn, fourni par l'administrateur réseau.

**Dans notre cas**, cliquer sur l'onglet **"UPLOAD FILE"**, afin de procéder à l'importation du fichier généré depuis pfSense. Ce fichier contient l'ensemble des informations nécessaires à la connexion sécurisée au serveur VPN (certificats, IP, port, mode d'authentification, etc.).





Cliquer sur Upload File

≡	Get conne	ected	10
	URL	UPLOAD FILE	٦
Type Server	Address or Cloud ID	<u> </u>	

#### Étape : ajout du profil VPN dans OpenVPN Connect

Une fois le client OpenVPN Connect lancé et l'onglet **"UPLOAD FILE"** sélectionné, il est possible d'importer le profil de connexion au serveur VPN.

Pour cela, effectuer un **glisser-déposer** du fichier .ovpn précédemment généré sur le bureau (dans notre cas : RTE01-UDP4-1194-config.ovpn) vers la zone centrale de l'interface, comme illustré ci-dessus.

🔎 Le fichier .ovpn contient l'ensemble des paramètres nécessaires pour établir une session VPN :

- L'adresse IP et le port du serveur distant,
- Les certificats d'authentification,
- Le mode de chiffrement et d'encapsulation,
- Les routes à appliquer une fois la connexion établie.

Remarque : un seul fichier .ovpn peut être importé à la fois.

Une fois le fichier déposé, le client OpenVPN Connect propose automatiquement de passer à l'étape de connexion en affichant un bouton **"Connect"**. Cette opération permet de tester la liaison avec le serveur VPN configuré sur pfSense.





#### Étape :

#### authentification de l'utilisateur

Une fois le fichier de configuration .ovpn importé dans le client **OpenVPN Connect**, la fenêtre **"Imported Profile"** s'affiche automatiquement. Celle-ci contient deux champs essentiels pour la phase d'authentification :

- Server Hostname : affiche l'adresse IP ou le nom DNS du serveur VPN (ici, 192.168.1.251). Cette valeur est verrouillée car elle provient du fichier de configuration.
- Username : ce champ doit être complété avec les identifiants d'un utilisateur du domaine Active Directory.

#### Dans notre cas :

Le nom d'utilisateur sera par exemple BTRINH, comme défini précédemment dans le gestionnaire d'utilisateurs de pfSense.

Il est également possible de cocher la case **"Save password"** si l'on souhaite que le mot de passe soit mémorisé pour les connexions futures (non recommandé sur des postes partagés ou sensibles).

#### Finaliser la connexion

Une fois les informations saisies, cliquer sur le bouton **"CONNECT"** afin d'établir la connexion VPN. Le client initiera alors une demande TLS vers le serveur OpenVPN, s'authentifiera à l'aide du certificat et des identifiants Active Directory, et établira un tunnel chiffré sécurisé.



Rentrer l'utrilisateur BTRINH créer auparavant via l'active directory

penvenco	
<	Imported Profile
Profile Name	3
192.168.1	.251 [RTE01-UDP4-1194-config (1)]
Server Host	name (locked)
192 168 1	.251

Après avoir cliqué sur **"CONNECT"**, une fenêtre s'affiche automatiquement demandant la **saisie du mot de passe** associé au **nom d'utilisateur précédemment renseigné**.

- **Profile** : identifie le profil de connexion utilisé (ici RTE01-UDP4-1194-config (1) pointant vers 192.168.1.251).
- **Password** : ce champ doit contenir le **mot de passe Active Directory** correspondant à l'utilisateur.

Enter passwo Profile: 192.168.1.251 [RTE01-U config (1)]	ord DP4-1194-
Password	B
ок	CANCEL

#### Dans notre cas :

Le mot de passe à saisir est celui associé à l'utilisateur **BTRINH**, tel que défini dans l'annuaire Active Directory. Une fois le mot de passe entré, cliquer sur **"OK"** pour procéder à l'authentification.

L'image ci-dessus confirme que **la connexion VPN a bien été établie** à l'aide du client **OpenVPN Connect** :

• Statut : CONNECTED  $\rightarrow$  L'utilisateur est désormais relié de

façon sécurisée au réseau distant via le tunnel VPN.

- **Profil utilisé** : 192.168.1.251 [RTE01-UDP4-1194-config (1)] (ce fichier de configuration .ovpn contient les informations nécessaires pour initier la session VPN).
- Données en transit :
  - Bytes In : données reçues depuis le serveur VPN (ici 370 B/s)
  - Bytes Out : données envoyées vers le serveur (ici 80 B/s)
- Identité utilisateur : BTRINH (authentifié via l'annuaire Active Directory).





La session VPN est **active** et **fonctionnelle**. Le poste client est désormais en mesure d'accéder aux ressources internes du réseau de l'entreprise (serveurs, partages, etc.), **comme s'il était physiquement connecté au LAN**.

Suite à la connexion réussie via le client **OpenVPN Connect**, des tests de connectivité ont été réalisés afin de s'assurer que la machine cliente peut bien accéder aux ressources du réseau distant via le tunnel VPN :

#### Test Ping réussi

Deux adresses IP ont été pingées avec succès depuis le client :

- 192.168.10.254  $\rightarrow$  Interface LAN du routeur distant (PfSense)
- 192.168.10.251 → Adresse d'un équipement ou serveur situé dans le réseau local distant

Dans les deux cas :

- Temps de réponse : 1 ms
- Paquets reçus : 100 %
- Aucune perte de paquets

La configuration du VPN Road Warrior avec authentification LDAP/Active Directory est **opérationnelle**, et la connectivité réseau est **confirmée** par ces tests. L'utilisateur distant peut désormais utiliser les services internes (AD, fichiers, imprimantes réseau, etc.).




### **Procédure d'utilisation VPN**

Pour établir une connexion VPN avec le serveur OpenVPN, l'utilisateur doit suivre les étapes ci-dessous : 1. Lancer l'application OpenVPN Connect



BTSSID

 Dans la barre des tâches de Windows (en bas à droite de l'écran), cliquer sur la flèche vers le haut ( \* étape 1 sur la capture) pour afficher les icônes cachées.

 Rechercher et cliquer sur l'icône d'OpenVPN Connect ( \* étape 2 sur la capture). Cette icône symbolise un casque avec un petit point rouge.

Cela permet d'ouvrir l'interface du client OpenVPN et de gérer les profils de connexion.

Une fois l'application **OpenVPN Connect** ouverte, l'utilisateur accède à l'interface de gestion des **profils VPN**.

### 2. Activer la connexion VPN

- L'utilisateur voit son profil VPN affiché liste (dans cet exemple : 192.168.1.251 UDP4-1194-config (1)]).
- Le statut affiché est **DISCONNECTED** (déconnecté).
- Pour se connecter, il suffit de cliquer sur l'interrupteur gris (encadré en rouge sur la capture) pour lancer la connexion.



Une fois l'interrupteur activé pour établir la connexion VPN, une **fenêtre de saisie du mot de passe** apparaît.



1. **Entrer le mot de passe associé au compte utilisateur** (dans cet exemple, le compte est BTRINH).

Ce mot de passe correspond à celui de l'annuaire Active Directory si l'authentification LDAP a été configurée.

2. **Cliquer sur OK** pour valider l'identification et établir la connexion VPN.

Si les identifiants sont corrects et que le serveur OpenVPN est fonctionnel, la connexion sera établie et le statut passera à **CONNECTED**.

### Connexion réussie

Une fois le mot de passe validé, la fenêtre suivante s'affiche indiquant que la **connexion VPN est établie avec succès**.

### Informations visibles :





• Statut : CONNECTED (en vert) confirme que le tunnel VPN est actif.

OpenVPN Connect - 2					
≡	Profiles	1			
CONNEC	CTED				
	OpenVPN Profile 192.168.1.251 [RTE01-UDP4- 1194-config (1)]				
CONNEC	CTION STATS				
3.7KB/s		_			
0B/s					
BYTES IN 481 B/S	↓ ↑ BYTES 165 B/S	OUT			
DURATION 00:00:0	N PACKET RECEIVED 5 3 sec ago				
YOU					
BTRINH					

Nom du profil : ici, 192.168.1.251 [RTE01-UDP4-1194-config (1)], qui correspond au fichier .ovpn importé. Statistiques de connexion : Débit entrant/sortant (BYTES IN / OUT) : données échangées en temps réel entre le client et le serveur.

**Durée** : temps écoulé depuis l'établissement de la connexion.

**Nom d'utilisateur** : l'utilisateur authentifié (ex. BTRINH dans cet exemple).

Vous êtes désormais connecté au réseau interne via le tunnel VPN. Vous pouvez accéder aux ressources du réseau distant (serveurs, partages, services internes) comme si vous étiez physiquement sur site.





### **Annexe : Glossaire des termes techniques**

### VM (Virtual Machine)

Une <u>machine virtuelle</u> est un système d'exploitation simulé dans un environnement logiciel comme VMware. Elle permet d'exécuter plusieurs OS sur un même ordinateur physique.

### VMware

VM ware est un logiciel d'hypervision qui permet de créer et gérer des machines virtuelles pour virtualiser des serveurs ou postes de travail.

### pfSense

pfSense est une distribution open source basée sur FreeBSD utilisée comme pare-feu, routeur, serveur VPN, etc.

### LAN / WAN / DMZ

- LAN (Local Area Network) : réseau interne de l'entreprise.
- WAN (Wide Area Network) : connexion vers Internet.
- <u>DMZ (Demilitarized Zone)</u> : zone tampon entre le LAN et Internet pour héberger des services publics (web, mail...).

### Interface réseau

Une <u>interface réseau</u> est une carte réseau virtuelle ou physique à laquelle est attribuée une adresse IP pour permettre la communication réseau.

### ZFS

<u>ZFS</u> est un système de fichiers moderne et fiable, utilisé par pfSense pour garantir l'intégrité des données. DHCP

Le <u>DHCP</u> est un protocole permettant d'attribuer automatiquement une adresse IP aux équipements connectés à un réseau.

### CARP (Common Address Redundancy Protocol)

CARP permet à deux routeurs pfSense de partager une adresse IP virtuelle et d'assurer une haute disponibilité.

### pfsync

pfsync permet de synchroniser les connexions actives entre deux pare-feux pour éviter les coupures lors d'un basculement.

### Failover

Le <u>failover</u> permet de basculer automatiquement vers une autre connexion ou un autre équipement en cas de panne.

### Load balancing

Le <u>load balancing</u> (répartition de charge) répartit le trafic réseau entre plusieurs connexions pour améliorer les performances et la redondance.

### **Gateway Group**

Un Gateway Group permet de regrouper plusieurs passerelles avec des priorités pour gérer le failover ou le load balancing dans pfSense.

### Pare-feu (Firewall)

Un <u>pare-feu</u> filtre les connexions réseau entrantes ou sortantes selon des règles. Il protège le réseau contre les attaques ou accès non autorisés.





### OpenVPN

BTSSID

<u>OpenVPN</u> est un protocole VPN open source qui crée un tunnel sécurisé entre un client et un réseau distant.

### Road Warrior

Road Warrior est une configuration VPN OpenVPN pour utilisateurs nomades, leur permettant de se connecter à distance au réseau d'entreprise.

### CA (Certificate Authority)

Une <u>autorité de certification (CA)</u> est une entité qui signe des certificats numériques, utilisés pour sécuriser et authentifier les connexions.

### Certificat serveur / utilisateur

Un <u>certificat numérique</u> contient des clés cryptographiques utilisées pour chiffrer les connexions (VPN, HTTPS...) et identifier les serveurs ou utilisateurs.

### LDAP (Lightweight Directory Access Protocol)

<u>LDAP</u> est un protocole permettant d'interroger un annuaire comme Active Directory pour authentifier des utilisateurs.

### Active Directory (AD)

<u>Active Directory</u> est un service d'annuaire Microsoft qui centralise la gestion des utilisateurs, groupes et ressources réseau.

### Tunnel VPN

Un <u>tunnel VPN</u> est une connexion sécurisée entre un utilisateur et un réseau distant, chiffrée pour garantir la confidentialité.

### TLS (Transport Layer Security)

<u>TLS</u> est un protocole de sécurité qui chiffre les communications entre deux systèmes (ex : VPN, HTTPS...). **Port 1194** 

Le port 1194 UDP est le port par défaut utilisé par OpenVPN pour accepter les connexions entrantes. **.ovpn** 

Un fichier .ovpn est un fichier de configuration OpenVPN contenant les paramètres nécessaires à la connexion VPN.

### **OpenVPN Client Export**

OpenVPN Client Export est un module pfSense qui permet d'exporter facilement des fichiers .ovpn pour les utilisateurs.

### Bind DN / Password

Le Bind DN est un identifiant utilisé par pfSense pour se connecter à un annuaire LDAP afin de vérifier les identifiants des utilisateurs.

### UDP / TCP

- <u>UDP</u> : protocole rapide sans vérification (utilisé pour VPN, jeux en ligne...).
- <u>TCP</u> : protocole fiable avec vérification (utilisé pour HTTP, FTP...).

### AES / SHA256 / CHACHA20

- <u>AES</u> : algorithme de chiffrement très sécurisé utilisé dans OpenVPN.
- <u>SHA256</u> : algorithme de hachage pour vérifier l'intégrité des données.
- <u>CHACHA20</u> : alternative performante à AES, notamment sur les processeurs sans accélération matérielle.



### Création, d'une VM sur VM WARE

Lorsque vous créer une machine virtuelle l'option « Typical (recommended) est cocher de base.





New Virtual Machine Wizard	×	
Name the Virtual Machine What name would you like to use for this virtual machine?		
SRV-VOIP		
E:\VM\BTS-SIO\AP4\RTE-01 Brov2e The default location can be changed at Edit > Preferences.		
< Back Next > 3.0		

Dans cette étape nous allons devoir nommer le serveur ainsi que choisir l'emplacement de la VM

- (1) Ensuite nous allons nommer le server
- (2) Choisir l'emplacement ou sera situé la VM

(3) Cliquer sur « Next » pour passer à la prochaine étape

Ensuite sur cette étape nous allons allouer l'espace du disque pour notre serveur. Dans notre cas il n'est pas nécessaire d'avoir un gros espace de stockage sur notre serveur.

Cliquer sur « Next » pour passer à la	New Virtual Machine Wizard X	
prochaine etape	Specify Disk Capacity How large do you want this disk to be?	
	The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.	
	Maximum disk <u>s</u> ize (GB):	
	Recommended size for Ubuntu: 20 GB	
	○ Store virtual disk as a single file	
	• Split virtual disk into multiple files	
	Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.	
Ensuite dans cette partie-là nous configurer les options suivantes :		allons
	Help < <u>B</u> ack <u>Next</u> > Cancel	

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 78 / 197 - CHAHROUR Walid









3) Récapitulatif de la configuration lu serveur.

(4) Cliquer sur « Finish » pour passer à la prochaine étape

Une fois avoir fini de vérifier les information du serveur, la VM ( Virtual Machine) va se créer ainsi vous pouvez le lancer.





### **Installation Débian 12.0**

L'écran affiché correspond au **menu principal du programme d'installation de Debian 12**, exécuté en mode BIOS. À cette étape, plusieurs options sont proposées à l'utilisateur pour initier l'installation du système d'exploitation.

L'option actuellement sélectionnée est :

**Graphical install** : cette méthode propose une installation assistée via une interface graphique conviviale, facilitant la configuration pour les utilisateurs non familiers avec l'environnement en ligne de commande.



Sélectionner Graphical install

Autres options disponibles :

• Install : installation en mode texte, adaptée aux environnements serveur ou aux

systèmes nécessitant une configuration légère sans interface graphique.

- Advanced options : permet d'accéder à des paramètres spécifiques (ex. : expert install, mode rescue...).
- Accessible dark contrast installer menu : mode d'installation graphique avec un thème à contraste élevé, destiné à améliorer l'accessibilité visuelle.
- Help : documentation succincte sur les options d'installation.
- Install with speech synthesis : installation adaptée aux personnes malvoyantes, avec synthèse vocale activée.

### Sélection de la langue – Étape détaillée

L'image ci-dessus correspond à l'écran de sélection de la langue dans le programme d'installation de Debian 12.



Select a language				
Choose the language to language for the install Language:	o be used for the installation process. The selected language w led system.	/ill also be th	e default	
cinnese (simplineu)	• 平义间冲/			i
Chinese (Traditional)	- 中文(繁體)			l
Croatian	- Hrvatski			l
Czech	- Čeština		-	
Danish	- Dansk		=	
Dutch	- Nederlands			
Dzongkha	- Pizzi - Pizzi -			
English	- English			l
Esperanto	- Esperanto			l
Estonian	- Eesti			l
Finnish	- Suomi			l
French	- Français 1			l
Galician	- Galego			l
Georgian	- ქართული			l
German	- Deutsch			
			2	2
Screenshot		Go Back	Continue	

### Sélectionner la langue souhaitée :

Cliquer sur l'entrée « French – Français » afin de définir le français comme langue principale pour l'installation ainsi que pour le système une fois celui-ci installé.

 $1. \ \ \text{Valider le choix}:$ 

Cliquer sur le bouton **Continue** (en bas à droite) pour passer à l'étape suivante.

Remarque : La langue sélectionnée influencera également la disposition du clavier proposée, les formats de date/heure, et certaines préférences

régionales par défaut.

Cette étape permet d'adapter l'ensemble du processus d'installation à la langue de l'utilisateur, garantissant ainsi une meilleure lisibilité et une configuration personnalisée.

### Choix de la situation géographique

Cette étape consiste à sélectionner le **pays de résidence** ou la **zone géographique** dans laquelle le système sera utilisé.

#### Objectif :

Le pays sélectionné permet à l'installeur de :

- Définir automatiquement le fuseau horaire,
- Appliquer les paramètres régionaux appropriés (format de date, heure, devise, etc.),
- Adapter certaines **préférences linguistiques** si nécessaire.

- Sélection de la région : L'utilisateur a ici sélectionné France comme situation géographique (étape 1) sur la capture).
- Validation de l'étape : Cliquer sur le bouton Continuer (étape 2) pour valider la sélection et poursuivre l'installation.

Cette étape est essentielle pour assurer le bon fonctionnement des paramètres régionaux du système Debian une fois installé.

e pays choisi permet de définir le fuseau ho « locale »). C'est le plus souvent le pays où	praire et de déterminer les paramètres régionaux du système vous vivez.
a courte liste affichée dépend de la langue	précédemment choisie. Choisissez « Autre » si votre pays n'est
pas affiché.	
Pays (territoire ou region) :	
Belgique	
Canada	
France 1	
Luxembourg	
Suisse	
Autre	
Capture d'écran	Revenir en arrièr 2 Continuer







#### Configuration du clavier

Cette étape permet de définir la **disposition du clavier** utilisée pendant l'installation et après l'installation du système Debian.

Le choix de la disposition clavier permet :

- D'assurer la correspondance entre les touches physiques et les caractères affichés,
- D'éviter les erreurs de saisie lors de la configuration (notamment pour les mots de passe),
- D'adapter l'environnement de travail à la langue et au matériel utilisés par l'utilisateur.

### Détail des actions visibles à l'écran :

Disposition de clavier à utiliser :	
Danois	-
Néerlandais	
Dvorak	
Dzongkha	-
Espéranto	100
Estonien	
Éthiopien	=
Finnois	
Français 1	
Géorgien	
Allemand	
Grec	20
Gujarati	1.1
Gourmoukhî	
Hébreu	
Hindi	
Hongrois	2

### 1. Sélection de la disposition :

L'utilisateur a sélectionné **Français** comme disposition clavier (étape 1) sur la capture). Cette option correspond à une disposition **AZERTY**, standard sur les claviers utilisés en France.

### 2. Validation de l'étape :

Cliquer sur le bouton **Continuer** (étape 2) pour confirmer la sélection et passer à l'étape suivante de l'installation.



### Configuration du réseau – Attribution d'une adresse de lien local (link-local)

Suite à l'échec de la détection d'une configuration via DHCP, l'installeur tente de configurer automatiquement une **adresse IP de lien local** pour permettre une connectivité minimale.

L'adresse de lien local (appelée aussi **link-local**) permet à un équipement réseau de s'auto-attribuer une adresse IP dans la plage **169.254.0.0/16** lorsqu'aucun serveur DHCP n'est disponible. Cela peut temporairement permettre des communications locales (entre machines connectées directement).

- Le système affiche le message :
   « Attente de l'adresse du lien local ("link-local")... »
   Cela signifie que Debian tente d'attribuer une adresse IP automatique sans dépendre d'un serveur.
- Cliquer sur le bouton « Annuler » permet d'interrompre ce processus si vous souhaitez configurer l'adresse réseau manuellement.

Configurer le réseau		
	Attente de l'adresse du lien local (« link-local »)	
		Annulor
		Annuler

### Configuration du réseau – Échec de l'attribution automatique (DHCP)

À cette étape, le programme d'installation tente de configurer automatiquement l'interface réseau via le protocole DHCP (Dynamic Host Configuration Protocol). Toutefois, une erreur s'est produite.

Cette phase a pour but d'obtenir automatiquement une adresse IP ainsi que les informations réseau nécessaires (passerelle, DNS) depuis un serveur DHCP, généralement présent sur le réseau local. Informations affichées à l'écran :

Le message indique que la configuration automatique a échoué. Les causes possibles incluent :

• L'absence de serveur DHCP sur le réseau,



- Un délai de réponse anormalement long du serveur DHCP,
- Une mauvaise détection ou défaillance matérielle de l'interface réseau.

Configurer le réseau La configuration automatique a échoué Le protocole DHCP n'est probablement pas utilisé sur le réseau. Il est également possible que le serveur DHCP soit lent ou que certains équipements réseau ne fonctionnent pas correctement.	Cliquer sur le bouton     "Continuer" pour poursuivre     l'installation et configurer     manuellement les paramètres     réseau lors de l'étape suivante.
Capture d'écran Continuer	

### Configuration du réseau – Choix de la méthode

Cette étape permet à l'utilisateur de définir **comment le réseau sera configuré**, suite à l'échec des tentatives automatiques via DHCP.

Déterminer manuellement ou automatiquement les paramètres réseau pour permettre au système de communiquer avec l'extérieur ou le réseau local.

Configurer le réseau	
Vous pouvez maintenant réessayer la configuration DHCP met du temps à répondre -, ou bien vous pou DHCP demandent qu'un hôte DHCP soit donné par l configuration automatique.	automatique du réseau, - cela peut réussir si le serveur vez configurer vous-même le réseau. Certains serveurs e client, vous pouvez l'indiquer avant de réessayer la
Méthode pour la configuration du réseau :	
Réessayer la configuration automatique du réseau	
Réessayer la configuration automatique avec un no	m d'hôte DHCP
Configurer vous-même le réseau	
Ne pas configurer le réseau maintenant	
Capture d'écran	Revenir en arrière Continuer

 Sélection de la méthode de configuration – repère ① :
 L'utilisateur a sélectionné l'option «
 Configurer vous-même le réseau », ce qui permet de définir manuellement les paramètres réseau tels que :

- o l'adresse IP,
- o le masque de sous-réseau,
- la passerelle,
- et les serveurs DNS.

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 86 / 197 - CHAHROUR Walid





 Validation de l'étape – repère (2) : Cliquer sur « Continuer » permet d'accéder à l'assistant de configuration manuelle.

### Autres options proposées :

- **Réessayer la configuration automatique** : utile si le serveur DHCP était temporairement inaccessible.
- **Réessayer avec un nom d'hôte DHCP** : certains serveurs DHCP nécessitent un nom d'hôte pour attribuer une adresse.
- Ne pas configurer le réseau maintenant : à éviter dans la majorité des cas, sauf si l'accès réseau est volontairement désactivé (par exemple en environnement isolé ou test local).

### onfiguration du réseau – Définition manuelle de l'adresse IP

Dans cette phase, l'utilisateur est invité à **saisir manuellement l'adresse IP** qui sera attribuée à l'interface réseau principale de la machine.

L'adresse IP permet à la machine Debian d'être identifiée sur le réseau local. Cette étape est essentielle dans une configuration réseau statique (absence de DHCP).

### Détail des actions visibles à l'écran :

Saisie de l'adresse IP – repère (1)
 :

L'utilisateur a saisi l'adresse IP 192.168.10.60, qui correspond à l'IP statique prévue pour le serveur nommé SRV-VOIP dans l'infrastructure cible.

Validation de l'adresse – repère
 :

Cliquer sur **« Continuer »** permet de confirmer cette adresse IP et de passer à l'étape suivante (masque de sous-réseau).

L'adresse IP est pr	opre à une machin	e et peut être const	ituée de :		
* quatre nombres * des blocs de car « deux-points »	séparés par des po actères hexadécim IPv6).	oints (IPv4) ; aux séparés par le c	aractère		
ll est également pe	ossible d'ajouter u	n masque de sous-re	éseau au format CIDR	(par exemple « )	/24 »).
Si vous ne savez p Adresse IP : IP de	as quoi indiquer, v e votre SRV-VC	euillez consulter l'a	dministrateur de voti	re réseau.	
192.168.10.60					

Cette adresse doit impérativement appartenir au même sous-réseau que les autres équipements du réseau local, et être **unique** pour éviter les conflits IP.



### Configuration du réseau – Définition du masque de sous-réseau

Après la saisie de l'adresse IP, cette étape permet de renseigner le **masque de sous-réseau**, paramètre indispensable pour déterminer l'étendue du réseau local. **Objectif :** 

Le masque de sous-réseau permet de :

- Identifier quelles adresses IP sont considérées comme locales (dans le même réseau),
- Définir la taille du réseau (nombre d'hôtes disponibles),
- Assurer une communication efficace entre les machines du même sous-réseau.

#### Exemple utilisé :

Dans la capture, l'utilisateur a saisi :

**255.255.255.0**, ce qui correspond au préfixe **/24**, soit un réseau contenant jusqu'à **254 hôtes utilisables** (de 192.168.10.1 à 192.168.10.254).

e masque-réseau sert à déterminer les mach onsultez votre administrateur. Le masque-ré 'aleur du masque-réseau :	ines locales du résea seau est une série d N	au. Si vous ne connaissez pa e quatre nombres séparés p	s cette valeur, ar des points.
55.255.255.0			
anture d'écran		Bevenir en arrière	Continuer

Cliquer sur **« Continuer »** pour valider le masque et poursuivre la configuration réseau (passerelle par défaut).

### Configuration du réseau – Définition de la passerelle (routeur par défaut)

Une fois l'adresse IP et le masque de sous-réseau définis, cette étape permet d'indiquer la **passerelle par défaut**, c'est-à-dire l'adresse IP du routeur par lequel transite tout le trafic sortant du réseau local.





La passerelle est utilisée pour :

- Accéder à d'autres réseaux, y compris Internet, ٠
- Acheminer les paquets destinés à des adresses extérieures au sous-réseau local,
- Garantir la connectivité complète d'un serveur ou d'un poste de travail. ٠

Détail des actions visibles à l'écran :

1.	Saisie de l'adresse IP du	Configurer le réseau	routeur –
	repère ① :	La passerelle est une adresse IP (quatre nombres séparés par des points) qui indique la machine qui joue le rôle de routeur ; cette machine est aussi appelée le routeur par défaut. Tout le trafic qui sort du réseau (p. ex.	
	L'utilisateur a saisi	vers Internet) passe par ce routeur. Dans quelques rares circonstances, vous n'avez pas besoin de routeur. Si c'est le cas, vous pouvez laisser ce champ vide. Consultez votre administrateur si vous ne connaissez pas la réponse correcte à cette question.	
	192.168.10.254, adresse IP	Passerelle : 192.168.10.254   IP de votre routeur	
	typiquement utilisée pour		
	représenter l'interface LAN		d'un
	routeur (dans cet exemple,		
	probablement l'adresse		LAN d'un
	pare-feu pfSense).		
2.	Validation de l'étape –	2	repère
	2 :	Capture d'écran Revenir en arrière Continuer	Cliquer
	sur <b>« Continuer »</b> permet		de

sur « Continuer » permet

confirmer la passerelle et de passer à la configuration des serveurs DNS.

#### Configuration du réseau – Définition des serveurs DNS

Lors de cette étape, l'installateur Debian demande à l'utilisateur de renseigner les adresses IP des serveurs DNS qui seront utilisés pour la résolution de noms de domaine (traduction d'un nom comme srvvoip.cod.lan en adresse IP).

Les serveurs DNS permettent :

- La résolution des noms d'hôtes en adresses IP sur le réseau local ou Internet,
- Le bon fonctionnement des services réseau nécessitant une communication par nom (Active Directory, messagerie, accès web, etc.),

Epreuve E6 – Situation professionnelle 2 - Documentation Technique - Page 89 / 197 - CHAHROUR





• Une gestion centralisée des ressources via les FQDN (noms complets de machines).



 Saisie des adresses IP des serveurs DNS – repère ①:
 L'utilisateur a renseigné deux adresses

192.168.10.10 : correspond au serveur
AD1 (Active Directory principal),
192.168.10.30 : correspond au serveur
AD2 (ou un serveur secondaire gérant également le rôle DNS).
Ces deux serveurs doivent être configurés pour répondre aux requêtes DNS internes à l'organisation (et potentiellement faire du "forwarding" vers Internet).

2. Validation de l'étape – repère (2) :

Cliquer sur **« Continuer »** permet de valider les serveurs DNS et d'enregistrer la configuration réseau complète.





### Configuration du réseau - Nom de machine (hostname)

Dans cette étape, l'installateur Debian demande à l'utilisateur de définir un **nom d'hôte**. Il s'agit d'un identifiant unique utilisé pour nommer la machine sur le réseau.

Le nom d'hôte permet :

- D'identifier facilement le serveur dans l'infrastructure réseau,
- De faciliter la résolution DNS et l'intégration dans un domaine Active Directory,
- D'assurer la lisibilité dans les journaux systèmes, les services réseau, et les interfaces de supervision.

Configurer le réseau	
Veuillez indiquer le nom de ce système. Le nom de machine est un mot unique qui identifie le systèr	ne sur le réseau. Si vous ne connaissez pas ce
nom, demandez-le à votre administrateur réseau. Si vous in	stallez votre propre réseau, vous pouvez mettre ce
Nom de machine :	
SRV-VOIP 1	
	2
Capture d'écran	Revenir en arrière Continuer

1. Saisie du nom d'hôte – repère ① : L'utilisateur a défini le nom de la machine comme SRV-VOIP. Ce nom est explicite : il indique qu'il s'agit d'un serveur de téléphonie IP (Voice Over IP).

Il est recommandé d'utiliser une convention de nommage claire (ex. SRV-ROLE-SITE, comme SRV-AD-STG01 ou SRV-WEB-DMZ).

2. Validation de l'étape – repère (2) : Cliquer sur « Continuer » permet de confirmer le nom et de passer à la configuration du domaine.

### Configuration du réseau – Domaine

Lors de cette étape, l'installeur Debian propose généralement de définir un **nom de domaine** afin de compléter le nom d'hôte du serveur (FQDN). Cependant, **dans le cadre de cette installation**, **aucun nom de domaine n'a été spécifié**, et le champ a volontairement été laissé vide.

Le nom de domaine est habituellement utilisé pour :

• Intégrer le système dans un réseau d'entreprise structuré,

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 91 / 197 - CHAHROUR



- Permettre une résolution DNS cohérente entre les hôtes,
- Créer un FQDN du type nom-machine.domaine.local.

### Justification :

Dans ce cas précis, le domaine n'a pas été renseigné car :

- Le serveur n'est pas encore intégré à un domaine Active Directory,
- L'utilisation de FQDN n'est pas requise pour les services prévus,
- Le réseau local repose actuellement sur une résolution d'hôtes manuelle ou par DNS local préconfiguré.

•	le champ "Domaine" a été
	laissé <b>vide</b> .

 L'utilisateur a cliqué sur «
 Continuer » pour valider cette étape et poursuivre l'installation.

Configurer le réseau		
Le domaine est la partie de l'adresse Internet qui est par .com, .net, .edu, ou .org. Si vous paramétrez vot mais assurez-vous d'employer le même nom sur toute Domaine :	à la droite du nom de machine. Il se ter re propre réseau, vous pouvez mettre c es les machines.	mine souvent e que vous voulez
	()	
Capture d'écran	Revenir en arrière	Continuer





### Création du mot de passe superutilisateur (root)

Cette étape permet de définir un mot de passe sécurisé pour le **compte superutilisateur** (également appelé **root**), qui possède tous les droits d'administration sur le système Debian.

Le mot de passe root est essentiel pour :

- Administrer le système,
- Installer ou supprimer des paquets,
- Modifier des fichiers sensibles (comme ceux de configuration réseau ou système),
- Intervenir en cas de panne ou de défaillance d'un utilisateur.

### Recommandations de sécurité :

- Le mot de passe doit contenir au minimum huit caractères.
- Il est recommandé d'inclure des majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Il ne doit pas être trop simple ou prévisible, ni réutilisé sur d'autres comptes ou systèmes.

Créer les utilisateurs et choisir les mots de passe				
Vous devez choisir un mot de passe pour le superutilisateur, le compte utilisateur malintentionné ou peu expérimenté qui aurait accès à ce co conséquence, ce mot de passe ne doit pas être facile à deviner, ni corre vous être facilement associé.	e d'administration du système. Un ompte peut provoquer des désastres. En respondre à un mot d'un dictionnaire ou			
Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.				
Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si du superutilisateur sera désactivé et le premier compte qui sera créé a privilèges du superutilisateur avec la commande « sudo ».	Si vous laissez ce champ vide, le compte aura la possibilité d'obtenir les			
Par sécurité, rien n'est affiché pendant la saisie.				
Mot de passe du superutilisateur (« root ») :				
•••••				
Afficher le mot de passe en clair				
Veuillez entrer à nouveau le mot de passe du superutilisateur afin de v Confirmation du mot de passe :	vérifier qu'il a été saisi correctement.			
•••••				
🗆 Afficher le mot de passe en clair				
	2			
Capture d'écran	Revenir en arrière Continuer			

 Saisie du mot de passe root dans le champ prévu (étape 1 sur la capture).

2. Confirmation du mot de passe en le saisissant une seconde fois.

 3. Validation en cliquant sur « Continuer » (étape
 2).

### Création d'un utilisateur standard

Cette étape permet la création d'un **compte utilisateur non privilégié**, destiné à un usage courant du système. Il s'agit d'une **bonne pratique de sécurité**, qui vise à séparer les actions administratives (réalisées avec le compte root ou via sudo) des usages classiques (navigation, bureautique, développement, etc.).

Créer un utilisateur personnel afin de :

- Travailler sans utiliser le compte root,
- Protéger le système contre les erreurs involontaires d'administration,

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 93 / 197 - CHAHROUR



- Permettre l'identification claire de chaque utilisateur du système.
- Saisie du nom complet de l'utilisateur (dans notre exemple, « billy ») dans le champ prévu à cet effet.
- Validation de l'étape en cliquant sur le bouton « Continuer ».

Un compte d'u superutilisate	utilisateur va être eur (« root »), pour	créé afin que vous l'utilisation coura	s puissiez dispose nte du système.	r d'un compte différent	de celui du
Veuillez indiq d'origine des propre nom e	uer le nom comple courriels émis ains st un bon choix.	t du nouvel utilisa i que dans tout pr	teur. Cette inforn rogramme qui affi	nation servira par exem che ou se sert du nom o	ple dans l'adresse omplet. Votre
Nom complet o	lu nouvel utilisateur	:			
billy					
Conturo diáo				Revenir en arrière	Continues





#### Définition de l'identifiant système (login)

Cette étape consiste à **attribuer un identifiant unique** au nouvel utilisateur. Cet identifiant, également appelé **login**, permet à l'utilisateur de se connecter à son compte sous Debian.

- Définir un identifiant conforme aux règles de nommage des utilisateurs sous Linux,
- Associer cet identifiant à un environnement utilisateur personnel,
- Permettre l'authentification lors des connexions locales ou distantes.

Créer les utilisateurs et choisir les mots de passe	
Veuillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.	
Identifiant pour le compte utilisateur :	
Capture d'écran Revenir en arrière Continuer	

1. **Saisie de l'identifiant** souhaité (dans cet exemple : billy) dans le champ dédié.

2. Validation de l'étape en cliquant sur le bouton « Continuer ».

#### Définir le mot de passe du nouvel utilisateur

Une fois le nom complet et l'identifiant utilisateur renseignés, cette étape permet de définir un **mot de passe sécurisé** pour le compte utilisateur nouvellement créé. Objectif :

- Assurer la protection du compte utilisateur par un mot de passe fort,
- Vérifier que le mot de passe est correctement saisi via une double confirmation.

#### Détail des actions visibles à l'écran :



Un bon mot de passe est composé de lettres régulièrement. Mot de passe pour le nouvel utilisateur :	s, chiffres et signes de ponctuation. Il devra en outre être changé
•••••	
Afficher le mot de passe en clair Veuillez entrer à nouveau le mot de passe p Confirmation du mot de passe :	0 our l'utilisateur, afin de vérifier que votre saisie est correcte.
· ·	

1. Saisie du mot de passe dans le champ prévu à cet effet, puis confirmation dans le second champ (étape ①).

2. Validation de l'étape en cliquant sur le bouton « Continuer » (étape (2)).

**Détection des disques et du matériel** Lors de cette étape, l'installateur Debian procède automatiquement à la **détection** 

des périphériques de stockage présents sur la machine. Cela inclut les disques durs, SSD, clés USB ou tout autre média de stockage.

- Identifier les disques disponibles afin de proposer les options de partitionnement adaptées,
- Déterminer la configuration matérielle nécessaire pour l'installation du système.
- Une barre de progression intitulée « Détection des disques et des autres périphériques » s'affiche, accompagnée du message « Détection du matériel. Veuillez patienter... », signalant que le système analyse le matériel présent.

ecte	r les disques
	Détection des disques et des autres périphériques
	Détection du matériel. Veuillez patienter

#### Partitionnement des disques

Cette étape permet de définir la manière dont les données seront réparties sur le

disque dur. Le programme d'installation Debian propose plusieurs méthodes de partitionnement, allant de l'automatique à la configuration manuelle avancée.

- Créer les partitions nécessaires à l'installation du système d'exploitation.
- Choisir une méthode adaptée selon le niveau de personnalisation souhaité.

Détail des actions visibles à l'écran :





Partitionner les disques
Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.
Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.
Méthode de partitionnement :
Assisté - utiliser un disque entier
Assisté - utiliser tout un disque avec LVM
Assisté - utiliser tout un disque avec LVM chiffré
Manuel
Capture d'écran Revenir en arrière Continuer

lorsque :

- Le disque est entièrement dédié à Debian,
- Aucune donnée importante ne doit être conservée sur ce disque (car il sera formaté).

#### Sélection du disque à partitionner

Après avoir choisi la méthode de partitionnement, l'installateur propose de sélectionner le disque physique sur lequel les partitions seront créées.

- Déterminer le support de stockage principal destiné à recevoir le système Debian. ٠
- S'assurer que l'espace disque sélectionné est disponible et que son utilisation ne compromettra • pas d'autres systèmes existants.

Détail des actions visibles à l'écran :

### 1. Méthode sélectionnée :

L'utilisateur a choisi l'option « Assisté – **utiliser un disque entier »** (étape (1) sur la capture), ce qui permet à l'installateur de gérer automatiquement la création des partitions standards.

#### 2. Validation de l'étape :

Cliquer sur le bouton Continuer (étape (2)) pour confirmer la méthode de partitionnement sélectionnée.

Cette méthode est recommandée pour une installation simple, notamment



1. Disque sélectionné :

Dans cet exemple, l'utilisateur a sélectionné le disque virtuel SCSI3 (0,0,0) (sda) – 21.5 GB VMware Virtual S, correspondant à un disque alloué dans un environnement VMware.

2. Validation de l'étape : Cliquer sur le bouton Continuer pour confirmer la sélection du disque et poursuivre le processus de partitionnement.

<b>euillez noter que toute ous souhaitez réelleme</b> Disque à partitionner :	es les données du di ent effectuer les moc	sque choisi seront lifications.	effacées mais pas avant	d'avoir confirmé que
SCS133 (0,0,0) (sda) - 2	1.5 GB VMware, VMw	vare Virtual S		

Attention : Toutes les données présentes sur ce disque seront supprimées. Cette opération est irréversible une fois validée.

### Choix du schéma de partitionnement

Une fois le disque sélectionné, l'assistant d'installation propose plusieurs méthodes de partitionnement en fonction de l'usage du système.

- Déterminer la manière dont les données seront organisées sur le disque dur.
- Adapter la structure du système de fichiers selon le niveau de compétence ou les besoins spécifiques de l'utilisateur.



Partitionner les disques
Disque partitionné :
SCSI33 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB
Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.
Schéma de partitionnement :
Tout dans une seule partition (recommandé pour les débutants)
Partition /home séparée
Partitions /home, /var et /tmp séparées
Capture d'écran Revenir en arrière Continuer

 Méthode sélectionnée : L'option Tout dans une seule partition (recommandé pour les débutants) est ici choisie (étape 1).

### 2. Validation de l'étape :

Cliquer sur le bouton **Continuer** (étape 2) pour confirmer le choix et passer à l'étape suivante.

Ce mode de partitionnement place l'ensemble des fichiers système, des données utilisateur et des journaux dans une seule partition (généralement /).

Avantages : simple à gérer, adapté aux environnements de test ou aux utilisateurs novices. Inconvénients : en cas de saturation du disque, cela peut impacter l'ensemble du système (pas d'isolation entre /home, /var, etc.).

### Validation du schéma de partitionnement

Cette étape permet de vérifier et de valider le plan de partitionnement du disque sélectionné avant de procéder à son application.

- Confirmer la structure des partitions définies précédemment.
- Écrire les modifications sur le disque pour permettre l'installation du système.

### Présentation de la table de partitions

Le système affiche les partitions créées :

- Une partition principale de type ext4, point de montage /, avec une taille de 20.4 Go.
- Une partition logique de type swap de 1.0 Go, utilisée comme mémoire d'échange.

Ces partitions sont listées sous le périphérique sélectionné :

SCSI3 (0,0,0) (sda) – 21.5 GB VMware, VMware Virtual S.

#### Action sélectionnée

L'utilisateur choisit l'option **Terminer le partitionnement et appliquer les changements**. Cette action est requise pour finaliser cette étape et initier la phase de formatage des partitions.





Continuer

#### Validation Partitionner les disques Cliquer sur le bouton Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions. **Continuer** pour confirmer ce Partitionnement assisté choix et passer à l'étape Configurer le RAID avec gestion logicielle suivante de l'installation. Configurer le gestionnaire de volumes logiques (LVM) Configurer les volumes chiffrés Configurer les volumes iSCSI SCSI33 (0.0.0) (sda) - 21.5 GB VMware, VMware Virtual S n° 1 primaire 20.4 GB f ext4 n°5 logique 1.0 GB f swap swap Annuler les modifications des partitions iner le partitionnement et appliquer les changen

Aide

### Confirmation de l'écriture des modifications sur le disque

À cette étape, le système demande une confirmation avant d'écrire définitivement les modifications sur le disque dur. Il s'agit d'une étape critique, car elle entraîne l'effacement complet des données précédemment présentes sur le disque sélectionné.

Capture d'écran

### Objectif :

• Autoriser le programme d'installation à formater les partitions et écrire la nouvelle table des partitions sur le disque.



# Choix de confirmation L'utilisateur a sélectionné l'option Oui (étape 1) pour autoriser l'application des changements.

Revenir en arrière

### 2. Validation

Cliquer sur le bouton **Continuer** (étape 2) permet de lancer effectivement le formatage et l'écriture sur le disque.



### Installation du système de base

Cette étape marque le début de l'installation effective du système Debian. Elle consiste à copier et configurer les fichiers essentiels au bon fonctionnement du système d'exploitation. **Objectif :** 

• Installer les composants de base nécessaires à l'exécution du système (bibliothèques, noyau, utilitaires de gestion, etc.).

### Détail des actions visibles à l'écran :

staller	r le système de base
	Installation du système de base
	Validation de libhogweed6

• Le système procède à l'**installation du système de base**, comme indiqué par la barre de progression.

• La mention « *Validation de libhogweed6…* » indique qu'un paquet spécifique est en cours de traitement.

### Configuration de l'outil de gestion des paquets

Lors de cette phase, l'installeur identifie le support d'installation utilisé et propose éventuellement d'ajouter d'autres sources pour la récupération des paquets logiciels.

- Valider le support d'installation principal contenant les paquets.
- Proposer à l'utilisateur d'ajouter des sources supplémentaires si nécessaire (ex : autre CD/DVD ou clé USB).

Le système détecte automatiquement le média d'installation en cours : **Debian GNU/Linux 12.10.0** *Bookworm* – Official amd64 NETINST with firmware 20250315-10:09. Le message indique que ce média sera utilisé pour l'installation des paquets via l'outil APT.



L'utilisateur sélectionne **Non** (étape (1)) car aucun support supplémentaire n'est requis dans ce contexte.

Configurer l'outil de gestion des paquets
L'analyse des supports d'installation a trouvé l'étiquette :
Debian GNU/Linux 12.10.0 _Bookworm Official amd64 NETINST with firmware 20250315-10:09
Vous pouvez maintenant analyser des médias supplémentaires qui seront utilisés par l'outil de gestion des paquets (APT). En principe, ils devraient appartenir au même ensemble que le média d'amorçage. Si vous n'avez pas d'autres supports disponibles, vous pouvez passer cette étape.
Si vous souhaitez analyser d'autres supports, veuillez en insérer un autre maintenant.
Faut-il analyser d'autres supports d'installation ?
O Oui
Capture d'écran Revenir en arrière Continuer

Cliquer sur le bouton **Continuer** (étape 2) permet de passer à l'étape suivante.

Cette étape est utile uniquement si vous disposez de plusieurs sources de paquets physiques. Dans la majorité des cas (comme ici), elle

peut être ignorée en toute sécurité.

#### Sélection du pays pour le miroir Debian

Cette étape permet de configurer le téléchargement des paquets via un **miroir réseau**. Un miroir Debian est un serveur contenant les fichiers nécessaires à l'installation et à la mise à jour du système.

- Choisir un pays géographiquement proche afin d'optimiser la rapidité des téléchargements.
- Faciliter la connexion à un miroir fiable et à jour.





- 1. Sélection du pays France dans la liste des miroirs disponibles (étape (1)).
- Valider la sélection en cliquant sur le bouton Continuer (étape 2).

L'objectif est de trouver un miroir de l'archi Gardez à l'esprit que le fait de choisir un pa choix.	ive Debian qui soit proche de vous du poin lys proche, voire même votre pays, n'est p	t de vue du réseau. eut-être pas le meilleur
Pays du miroir de l'archive Debian :		
Corée du Sud		(
Costa Rica		
Croatie		
Danemark		
Espagne		
Estonie		
Finlande		
France 1		
Grèce		
Géorgie		
Hong Kong		
Hongrie		
Inde		
Indonésie		
Iran		
		2
Capture d'écran	Revenir en arri	ère Continuer





#### Sélection du miroir Debian

Une fois le pays sélectionné, l'installeur propose une liste de **miroirs** disponibles dans la région. Ces miroirs sont des serveurs hébergeant les fichiers nécessaires à l'installation et à la mise à jour du système Debian.

### Objectif :

- Choisir un miroir fiable et performant pour télécharger les paquets via le gestionnaire APT.
- Optimiser la vitesse d'installation et de mise à jour.

#### Détail des actions visibles à l'écran :

Veuillez choisir un miroir de l'archive Debian. Vo région si vous ne savez pas quel miroir possède l	us devriez utiliser un miroir situé dans votre pays ou votre la meilleure connexion Internet avec vous.
Généralement, deb.debian.org est un choix pert	inent.
Miroir de l'archive Debian :	
deb debian org	
ta fr debian era	
debian proved pet	
debian.proxad.net	
ntp.ec-m.tr	
deb-mir1.naitways.net	
miroir.univ-lorraine.fr	
ftp.u-picardie.fr	
ftp.u-strasbg.fr	
mirror.plusserver.com	
debian.univ-tlse2.fr	
ftp.univ-pau.fr	
mirrors.ircam.fr	
ftn lin6 fr	
debian nebutech lille fr	
debian.polytech-inte.n	2
Construct different	
Capture d'ecran	Revenir en arrière Continuer

1. Sélection du miroir **deb.debian.org**, recommandé par défaut pour sa stabilité et sa répartition mondiale (étape (1)).

2. Cliquer sur **Continuer** pour valider le choix et passer à l'étape suivante (étape (2)).

#### Configuration d'un mandataire HTTP (proxy)

Dans cette étape, le programme d'installation propose d'indiquer un mandataire HTTP (également appelé proxy) si l'accès à Internet est restreint dans l'environnement réseau. **Objectif :** 

• Permettre à l'outil APT de télécharger les paquets via un serveur mandataire, si nécessaire.

#### Situation spécifique :

Dans le cadre de cette installation, **aucun proxy n'est requis**. Le champ « Mandataire HTTP » est donc **laissé vide**.





Laisser le champ de saisie vide, car aucune configuration proxy n'est nécessaire. Cliquer sur **Continuer** pour valider et passer à l'étape suivante.

**Remarque** : Cette étape est optionnelle et ne bloque pas l'installation si elle est ignorée.

xtérieur, indiquez ses paramètres ic	lataire HTTP (souvent . Sinon, laissez ce cha	: appelé « proxy ») pour accé mp vide.	der au monde
es paramètres du mandataire doiver basse]@]hôte[:port]/ ».	t être indiqués avec l	a forme normalisée « http://	[utilisateur][:mot-de-
Mandataire HTTP (laisser vide si aucun) :			

### Téléchargement des fichiers de configuration APT

Une fois le miroir Debian sélectionné et, le cas échéant, le mandataire HTTP configuré (ou laissé vide si inutile), l'installateur procède automatiquement à la configuration de l'outil de gestion des paquets APT.

- Télécharger les fichiers nécessaires à la gestion des paquets Debian.
- Préparer l'environnement pour l'installation des paquets supplémentaires.

Configurer l'outil de gestion des paquets
Configuration de l'outil de gestion des paquets (APT)
Téléchargement du fichier 7 sur 11
Annuler

• Une barre de progression indique l'état d'avancement du téléchargement (ici, fichier 7 sur 11).

• Aucun paramètre n'est requis de la part de l'utilisateur à cette étape.

**Remarque** : Cette opération peut prendre plusieurs minutes selon la vitesse de connexion Internet et la réactivité du miroir sélectionné. **Configuration de popularity-contest** Cette étape propose à l'utilisateur de participer à une étude statistique

anonyme sur l'utilisation des paquets Debian installés.





Permettre à la communauté Debian de recueillir des données d'usage réelles afin de :

- Mieux prioriser les paquets utilisés sur les supports d'installation,
- Améliorer l'optimisation de distribution.
- Dans ce cas précis, l'option sélectionnée (voir capture
- Le système n'enverra donc donnée statistique aux Debian.

Configuration de popularity-contest	les plus
Le système peut envoyer anonymement aux responsables de la distribution des statistiques sur les paquets que vous utilisez le plus souvent. Ces informations influencent le choix des paquets qui sont placés sur le premier CD de la distribution.	
Si vous cinoisissez de participer, un script enverra automatiquement chaque semaine les statistiques aux responsables. Elles peuvent être consultées sur https://popcon.debian.org/.	
Vous pourrez à tout moment modifier votre choix en exécutant « dpkg-reconfigure popularity-contest ». Souhaitez-vous participer à l'étude statistique sur l'utilisation des paquets ?	la
• Non	
O Oui	
	<b>"Non"</b> est
	d'écran).
	aucune
	serveurs
Capture d'écran Revenir en arrière Continuer	

### Informations complémentaires :

• En cas de changement d'avis, il est possible de reconfigurer cette option ultérieurement à l'aide de la commande :

### Sélection des logiciels à installer

À ce stade, seul le système de base est installé. L'installeur propose d'ajouter des ensembles de logiciels prédéfinis en fonction de l'usage prévu du système.

#### Objectif :

Permettre à l'utilisateur de choisir les composants à installer selon le rôle futur de la machine.

Sélection des logiciels		
Actuellement, seul le système de base es choisir d'installer un ou plusieurs ensemt Logiciels à installer :	t installé. Pour adapter l'installation à vos besoins, v oles prédéfinis de logiciels.	ous pouvez
<ul> <li>environnement de bureau Debian</li> <li> GNOME</li> </ul>	Décocher les deux cases	
<ul> <li> Xfce</li> <li> bureau GNOME Flashback</li> </ul>		
KDE Plasma     Cinnamon		
MATE     LXDE		
LXQt     serveur web		
<ul> <li>✓ serveur SSH</li> <li>✓ utilitaires usuels du système</li> </ul>		
Capture d'écran		Continuer

### 1. Désélection de l'environnement graphique :

Les cases « **environnement de bureau Debian** » et ses variantes (GNOME, KDE, etc.) sont **décochées** afin d'obtenir une installation **minimaliste en mode texte**, adaptée à un usage serveur ou à une configuration personnalisée.

2. Activation du serveur SSH : La case « serveur SSH » est cochée, ce qui permet l'accès distant sécurisé à la machine via le protocole SSH.

#### 3. Utilitaires usuels du système :

Cette option est cochée par défaut et **conservée** pour garantir l'installation d'outils de base nécessaires au bon fonctionnement du système Debian.

#### Résultat attendu :

À la fin de cette étape, le système sera installé sans interface graphique, mais avec les utilitaires essentiels et un accès distant possible via SSH.

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 106 / 197 - CHAHROUR



### Téléchargement et installation des logiciels sélectionnés

Une fois les options de logiciels validées (serveur SSH + utilitaires système), l'installeur Debian procède automatiquement à leur **téléchargement** et à leur **installation**. **Objectif :** 

Installer les paquets nécessaires au bon fonctionnement du système, en fonction des choix faits à l'étape précédente.

- Une barre de progression permet de suivre l'état d'avancement.
- L'indicateur « Téléchargement du fichier X sur Y » informe du nombre de paquets en cours de traitement.

Chaisis et in the land		
Choisir et installer des logio	leis	
	Choisir et installer des logiciels	
Téléchargement du fi	chier 26 sur 127	
reservingenene aa n		

### À savoir :

- Cette étape peut durer plusieurs minutes selon la vitesse de connexion Internet.
- Aucune intervention manuelle n'est nécessaire à ce stade.





### Installation du programme de démarrage GRUB

Cette étape permet d'installer le chargeur d'amorçage GRUB, nécessaire pour démarrer le système Debian installé.

#### Objectif :

Installer **GRUB** sur le disque principal, afin que l'ordinateur puisse démarrer automatiquement sur le nouveau système Debian.

Installer le programme de démarrage GRUB	1. L'option Oui est
Il semble que cette nouvelle installation soit le seul système d'exploitation existant sur cet ordinateur. Si c'est bien le cas, il est possible d'installer le programme de démarrage GRUB sur le disque principal (partition UEFI ou secteur.ld'amorçage). Attention : si le programme d'installation ne détecte pas un système d'exploitation installé sur l'ordinateur, cela empêchera temporairement ce système de démarrer. Toutefois, le programme de démarrage GRUB pourra être manuellement reconfiguré plus tard pour permettre ce démarrage. Installer le programme de démarrage GRUB sur le disque principal ?	sélectionnée (par défaut), car il s'agit de la seule installation présente sur l'ordinateur.
○ Non	2. Cliquer sur <b>Continuer</b> pour valider et poursuivre l'installation.
Capture d'écran Revenir en arrière Continuer	À savoir : • GRUB est indispensable pour que le système soit
	amorçable.

- Si aucun système n'est détecté, Debian considère que GRUB doit être installé.
- En cas de multi-boot, une configuration plus avancée pourrait être requise.




### Choix du périphérique d'installation de GRUB

Cette étape consiste à spécifier **sur quel disque** sera installé le chargeur d'amorçage GRUB, afin de rendre le système bootable.

### Objectif :

Installer **GRUB** sur le disque principal (/dev/sda) pour garantir que Debian se lance automatiquement au démarrage de la machine.

### Détail de l'écran :

- L'utilisateur sélectionne correspondant au principal (étape
- Cliquer sur pour valider ce finaliser l'installation de (étape 2).



### Remarques :

/dev/sda est

généralement le premier disque détecté, utilisé pour l'amorçage.

- Il est essentiel de ne pas confondre avec une partition spécifique comme /dev/sda1.
- Ce choix assure un démarrage automatique sans intervention manuelle après redémarrage.





### Installation de GRUB

### Objectif :

Finaliser l'installation du gestionnaire de démarrage **GRUB** afin de permettre le lancement de Debian automatiquement au démarrage du PC.

Installer le programme de démarrage GRUB					
Installation du programme de démarrag <mark>e GRUB</mark>					
Exécution de « update-grub »					

- Une **barre de progression** indique l'installation en cours du programme de démarrage.
- Le message « Exécution de update-grub... » confirme que GRUB est mis à jour pour reconnaître les systèmes installés.

### Remarques :

- Cette opération est automatique et ne nécessite pas d'intervention.
- À la fin de cette étape, le système est prêt à démarrer normalement depuis le disque principal.

### Terminer l'installation

Finaliser le processus d'installation de Debian et redémarrer sur le nouveau système.



- Le message confirme que l'installation est complète.
- Il est demandé de retirer support d'installation (clé etc.) avant de continuer, éviter de relancer l'installation au redémarrage.
- Cliquer sur le bouton
   Continuer déclenchera le redémarrage de la machine.

	nstallation terminée	
U L v é	'installation est terminée et vous allez pouvoir maintenant démarrer le nouveau système. Veuillez érifier que le support d'installation est bien retiré afin que le nouveau système puisse démarrer et viter de relancer la procédure d'installation.	
v	euillez sélectionner <continuer> pour redémarrer.</continuer>	
		le
		USB, C
		pour

Parfait ! Ce dernier écran indique que le système **Debian 12 a démarré correctement**. Tu arrives sur l'invite de connexion en mode console (TTY1), ce qui signifie que :



• L'installation s'est bien déroulée

• Le nom de la machine est bien SRV-VOIP (comme défini pendant l'installation)

### **Connexion à la machine**

La machine SRV-VOIP, fraîchement installée sous Debian GNU/Linux 12, est désormais opérationnelle. Voici les points clés vérifiés :

- Adresse IP attribuée : 192.168.10.60/24
- Passerelle par défaut : 192.168.10.254
- Résolution DNS : assurée via les serveurs internes 192.168.10.10 et 192.168.10.30
- Connexion Internet : testée avec succès par un ping vers 8.8.8.8 (0 % de perte de paquets)

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 111 / 197 - CHAHROUR



### La connectivité réseau est donc fonctionnelle et stable.

BTSSID

root@SV-V0IP: "/ ip a				
1: lo: <loopback,up,lower_up> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000</loopback,up,lower_up>				
link/loopback 00:00:00:00:00:00 brd 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: ens33: <broadcast,multicast,up,lower_up> mtu 1500 qdisc fq_codel state UP group default qlen 1000</broadcast,multicast,up,lower_up>				
link/ether 00:0c:29:25:09:72 brd ff:ff:ff:ff:ff				
altname enp251				
inet 192.168.10.60/24 Drg 192.168.10.255 Scope global ens33				
valio_itt torever preterred_itt torever				
ulid If foreign preferred Life foreign				
PINC 8 8 8 8 8 8 8 8 9 55(84) butes of data				
64 butes from 8.8.8.8' iron sec-1 +1-127 time-10.6 ms				
64 butes from 8.8.8.8; iron sec2 ttl=127 time=12.4 ms				
64 butes from 8.8.8.8; icmo seca ttl=127 time=11.0 ms				
64 bytes from 8.8.8.8: icmp sea=4 ttl=127 time=10.9 ms				
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=11.1 ms				
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=10.9 ms				
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=10.8 ms				
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=10.9 ms				
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=10.9 ms				
64 bytes from 8.8.8.8: icmp_seq=10 ttl=127 time=12.8 ms				
64 bytes from 8.8.8.8: icmp_seq=11 ttl=127 time=11.0 ms				
64 bytes from 8.8.8.8: icmp_seq=12 ttl=127 time=10.6 ms				
64 bytes from 8.8.8.8: icmp_seq=13 ttl=127 time=12.3 ms				
64 bytes from 8.8.8.8: 1cmp_seq=14 ttl=12/ t1me=11.0 ms				
64 bytes from 8.8.8.8: 1cmp_seq=15 ttl=127 t1m==10.2 ms				
64 butes from 6.8.6.8; long_seq=10 ttl=127 time=10.2 ms				
64 butes from 6.8.8.9 line cost 1 till_set 1112 till=107 till=10.0 ms				
$04$ bytes from 0.0.00. Long_seq-10 tr1=127 time=10.8 mc				
64 but es from 8.8.8.8. i imm seq-20 +11-127 time-10.4 me				
64 butes from 8.8.8.8; irmn seq=21 +1=127 time=10.3 ms				
64 butes from 8.8.8.8; iron see22 til=127 time=10.6 ms				
64 butes from 8.8.8.8: icmp sea=23 ttl=127 time=10.9 ms				
64 bytes from 8.8.8.8: icmp_seq=24 ttl=127 time=18.2 ms				
64 bytes from 8.8.8.8: icmp_seq=25 ttl=127 time=12.3 ms				
8.8.8.8 ping statistics				
25 packets transmitted, 25 received, 0% packet loss, time 24052ms				
rtt min/avg/max/mdev = 10.232/11.302/18.206/1.563 ms				
root@SRV-VUIP:"# _				

#### Installation du paquet sudo

- Commande exécutée : apt install sudo -y
- Version installée : 1.9.13p3-1+deb12u1 (issue des dépôts Debian Bookworm)



• Espace disque utilisé : ~6,2 Mo

### Ajout user dans le groupe sudo dans Debian 12

Comme on le voit dans ton terminal, l'utilisateur billy a bien été ajouté au groupe sudo usermod -aG sudo billy





### Mise à jour du système et installation des dépendances sudo apt

### update && sudo apt upgrade -y

Cette commande est composée de deux instructions distinctes reliées par les symboles &&, ce qui indique que la seconde instruction (sudo apt upgrade -y) ne sera exécutée que si la première (sudo apt update) s'exécute correctement et sans erreur.



Permet
 d'exécuter la
 commande
 avec des
 privilèges
 administratifs
 (root). Cela est
 nécessaire car
 ces opérations
 touchent au

sudo :

système lui-même et nécessitent des droits spécifiques.

- apt update :
  - Met à jour la liste des paquets disponibles à partir des sources configurées dans le fichier /etc/apt/sources.list et du répertoire /etc/apt/sources.list.d/.
  - Télécharge uniquement les informations sur les dernières versions disponibles des paquets, sans modifier ni installer aucun paquet.
- apt upgrade -y :
  - Met à jour tous les paquets installés sur le système vers leur version la plus récente disponible dans les dépôts.
  - L'argument -y (yes) permet de répondre automatiquement « oui » à toutes les questions posées par le gestionnaire de paquets durant le processus d'installation, évitant ainsi une interaction manuelle.

Cela signifie que votre système est déjà totalement à jour à l'instant de l'exécution de cette commande, et aucune action supplémentaire n'était nécessaire.

Cette commande exécute une installation groupée de plusieurs paquets essentiels et de bibliothèques nécessaires au développement logiciel, notamment pour compiler et exécuter certaines applications sur Debian 12.

• sudo :





- Utilisé pour exécuter les commandes avec les droits administrateurs nécessaires à l'installation de paquets système.
- apt install -y :
  - o Installe les paquets spécifiés en argument.
  - Le paramètre -y automatise la réponse affirmative à toutes les questions posées lors de l'installation.
- Description des paquets installés :
  - build-essential : Méta-paquet regroupant les outils de base nécessaires à la compilation de logiciels (gcc, make, etc.).
  - **wget** : Outil permettant le téléchargement de fichiers depuis Internet via la ligne de commande.
  - curl : Outil en ligne de commande permettant d'effectuer des transferts de données avec des URL, notamment utile pour récupérer des fichiers ou interagir avec des API.
  - **libedit-dev** : Bibliothèque d'édition de lignes en mode interactif utilisée principalement pour gérer les interactions utilisateur en terminal.
  - o **libxml2-dev** : Bibliothèque permettant le traitement des documents XML.
  - uuid-dev : Bibliothèque permettant la création et gestion d'identifiants uniques universels (UUID).
  - libjansson-dev : Bibliothèque légère permettant l'encodage, le décodage et la manipulation de données JSON.
  - libsqlite3-dev : Bibliothèque de développement pour SQLite, une base de données embarquée légère.
  - **libssl-dev** : Bibliothèque de développement pour le chiffrement SSL/TLS, nécessaire à la sécurisation des communications réseau.
  - **ncurses-dev** : Bibliothèque permettant le développement d'interfaces utilisateur interactives en mode texte (TUI).



Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 114 / 197 - CHAHROUR Walid



### Téléchargement et extraction des sources d'Asterisk :

Téléchargement des sources :

cd /usr/src

sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-current.tar.gz

- cd /usr/src :
  - La commande cd signifie **Change Directory** (« changer de répertoire »).
  - Le chemin /usr/src est traditionnellement utilisé sur les systèmes Linux pour stocker le code source des applications ou modules destinés à être compilés depuis les sources.
- sudo wget :
  - Exécute le téléchargement avec des droits administrateurs (privilège root), nécessaire pour écrire dans le répertoire /usr/src.
  - wget est une commande permettant de récupérer du contenu depuis un serveur web via le protocole HTTP ou HTTPS.
- URL : http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-current.tar.gz
  - Ceci est l'adresse complète menant vers le serveur officiel d'Asterisk pour télécharger la dernière version stable actuelle (version 20) sous forme d'archive compressée au format .tar.gz.
- Archive .tar.gz :
  - Format combinant TAR (archive) et GZip (compression), largement utilisé sous Unix/Linux.
  - Elle contient les fichiers sources nécessaires pour compiler et installer l'application (ici : Asterisk).



sudo tar xvf asterisk-20-current.tar.gz







#### sudo :

• Utilisé afin d'exécuter la commande avec les privilèges administratifs requis pour l'extraction des fichiers dans un répertoire système (/usr/src).

tar :

• La commande tar (**tape archive**) est utilisée pour archiver et désarchiver des fichiers sous Unix/Linux.

### Arguments utilisés avec tar :

- **x** : (extract) extrait le contenu d'une archive.
- v : (verbose) affiche les détails de l'extraction à l'écran, fichier par fichier.
- **f** : (file) indique que l'on spécifie un fichier d'archive en particulier à manipuler.

### Nom de l'archive :

• asterisk-20-current.tar.gz : Archive compressée contenant les fichiers sources nécessaires à la compilation et l'installation du logiciel Asterisk, version 20.

Ces fichiers sont essentiels pour préparer l'environnement de compilation, examiner les notes de version et valider la conformité des licences avant installation.



# BTSSID Compilation d'Asterisk :

Préparation à la compilation :

cd asterisk-20\*/ sudo contrib/scripts/get mp3 source.sh

billy@SRV-VOIP:/usr/src\$ cd asterisk-20\*/
sudo contrib/scripts/get\_mp3\_source.sh
contrib/scripts/get\_mp3\_source.sh: 18: svn: not found
billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$ cd asterisk-20\*/
-bash: cd: asterisk-20\*/: Aucun fichier ou dossier de ce type
billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$

Dans cette capture d'écran, on observe deux problèmes distincts :

- Erreur lors de l'exécution du script get\_mp3\_source.sh
- Cette erreur indique que le programme svn (Subversion) n'est pas installé sur ton système Debian. Ce script utilise svn pour récupérer le support MP3 pour Asterisk.
- Solution : Installer subversion avec : sudo apt install subversion -y

### Problème de chemin (cd asterisk-20\*/ ne fonctionne plus) :

-bash: cd: asterisk-20\*/: Aucun fichier ou dossier de ce type Cette erreur survient car tu es déjà à l'intérieur du dossier nommé explicitement asterisk-20.13.0. Une fois dedans, le dossier asterisk-20\*/ n'existe plus.

### Suite des opérations après la correction du problème MP3 :

Étape suivante (Vérification et compilation) :

Cette commande vérifie que toutes les dépendances nécessaires sont présentes avant la compilation sudo ./configure





V-VOIP:/usr/src/asterisk-20.13.0\$ sudo ./configure checking build system type... x86\_64-pc-linux-gnu checking host system type... x86\_64-pc-linux-gnu checking for gcc... gcc checking whether the C compiler works... yes checking for C compiler default output file name... a.out checking for suffix of executables... checking whether we are cross compiling... no checking for suffix of object files... o checking whether the compiler supports GNU C... yes checking whether gcc accepts -g... yes checking for gcc option to enable C11 features... none needed checking for stdio.h... yes checking for stdlib.h... yes checking for string.h... yes checking for inttypes.h... yes checking for stdint.h... yes checking for strings.h... yes checking for sys/stat.h... yes

### checking for shalsum... /usr/bin/shalsum checking for openssl... /usr/bin/openssl checking for pkg-config... no configure: error: pkg-config not found billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$

Ce message d'erreur provient d'un script configure utilisé lors de la préparation d'une compilation logicielle (dans ce contexte, la préparation de la compilation d'Asterisk depuis ses sources).

- checking for pkg-config... no :
  - Le script vérifie la présence de l'outil pkg-config, essentiel à la compilation de certains logiciels. Cet outil permet de récupérer automatiquement les informations nécessaires sur les bibliothèques installées sur le système (chemins, dépendances, versions, etc.).
- configure: error: pkg-config not found :
  - Ce message indique clairement que l'outil requis (pkg-config) est absent du système, entraînant l'arrêt immédiat du script de configuration. Il est impératif d'installer cet outil avant de poursuivre le processus.

#### Solution immédiate (à exécuter maintenant) :

Installe pkg-config avec la commande suivante : sudo apt install pkg-config -y

- sudo :
  - Permet d'exécuter la commande avec des privilèges administratifs (nécessaire pour modifier des éléments système).
- apt install pkg-config -y :





- Lance l'installation du paquet logiciel **pkg-config** avec APT, le gestionnaire de paquets utilisé sur Debian.
- L'option -y valide automatiquement toutes les demandes durant l'installation, ce qui évite toute intervention manuelle.
- pkg-config :
  - Outil utilisé durant la compilation de logiciels, permettant de récupérer automatiquement les paramètres de compilation nécessaires à l'intégration de bibliothèques externes.

contrigure. error, prg-contrig not tound
billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$ sudo apt install pkg-config -y
Lecture des listes de paquets Fait
Construction de l'arbre des dépendances Fait
Lecture des informations d'état Fait
Les paquets supplémentaires suivants seront installés :
libpkgconf3 pkgconf pkgconf-bin
Les NOUVEAUX paquets suivants seront installés :
libpkgconf3 pkg-config pkgconf pkgconf-bin
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 105 ko dans les archives.
Après cette opération, 283 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libpkgconf3 amd64 1.8.1-1 [36,1 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 pkgconf-bin amd64 1.8.1-1 [29,5 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 pkgconf amd64 1.8.1-1 [25,9 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 pkg-config amd64 1.8.1-1 [13,7 kB]
105 ko réceptionnés en 0s (866 ko/s)
Sélection du paquet libpkgconf3:amd64 précédemment désélectionné.
(Lecture de la base de données 42323 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de/libpkgconf3_1.8.1-1_amd64.deb
Dépaquetage de libpkgconf3:amd64 (1.8.1-1)
Sélection du paquet pkgconf-bin précédemment désélectionné.
Préparation du dépaquetage de/pkgconf-bin_1.8.1-1_amd64.deb
Dépaquetage de pkgconf-bin (1.8.1-1)
Sélection du paquet pkgconf:amd64 précédemment désélectionné.
Préparation du dépaquetage de/pkgconf_1.8.1-1_amd64.deb
Dépaquetage de pkgconf:amd64 (1.8.1-1)
Sélection du paquet pkg-config:amd64 précédemment désélectionné.
Préparation du dépaquetage de/pkg-config_1.8.1-1_amd64.deb
Dépaquetage de pkg-config:amd64 (1.8.1-1)
Paramétrage de libpkgconf3:amd64 (1.8.1-1)
Paramétrage de pkgconf-bin (1.8.1-1)
Paramétrage de pkgconf:amd64 (1.8.1-1)
Paramétrage de pkg-config:amd64 (1.8.1-1)
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2)
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u10)
billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$

Commandes à exécuter pour corriger immédiatement :

sudo apt install subversion -y

sudo contrib/scripts/get\_mp3\_source.sh

Installer Subversion (outil de gestion de version) et ses dépendances, nécessaires notamment pour récupérer le code source de modules ou plugins via des dépôts SVN.

Composants installés :

- Paquet principal :
  - $\circ$  subversion
- Dépendances :

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 119 / 197 - CHAHROUR



- libapr1
- o libaprutil1
- o libserf-1-1
- libsvn1
- libutf8proc2



Après avoir installé cette dépendance, relance à nouveau la commande : sudo ./configure

#### Explication des étapes clés :

- Vérification des dépendances :
  - $\circ$  checking for libxml2.0... yes → La bibliothèque libxml2 est détectée et disponible.
  - o checking for gtk+-2.0... no → La bibliothèque GTK+ 2.0 n'est pas présente, mais elle n'est pas indispensable pour la compilation standard d'Asterisk.
- Création des fichiers de configuration :
  - o config.status: creating makeopts → Génération du fichier contenant les options de compilation.
  - $\circ$  config.status: creating autoconfig.h → Génération d'un fichier d'en-tête utilisé pour adapter la compilation au système.



- Confirmation de configuration réussie :
  - configure: Menuselect build configuration successfully completed → Le système de configuration interne d'Asterisk (Menuselect) a été généré correctement. Ce composant permet de choisir les modules à inclure dans la compilation.

checking for libxml-2.0 ves					
checking for atk+-2.0 no					
configure: creating ./config.status					
config.status: creating makeopts					
config.status: creating autoconfig.h					
configure: Menuselect build configuration successfully	completed				
5 5 5					
.\$\$\$\$\$\$\$\$\$=					
.\$7\$77\$\$7:.					
.\$\$:. ,\$7.7					
.\$7. 7\$\$\$\$ .\$\$77					
\$\$. \$\$\$\$\$ .\$\$\$7					
7\$?\$\$\$\$\$?					
\$.\$\$\$\$7. \$\$\$\$7 .7\$\$\$\$\$\$.					
.777\$\$\$\$\$77\$\$\$77\$\$\$\$7.\$\$\$\$,					
\$\$\$~.7\$\$\$\$\$\$\$\$7\$\$\$.					
.\$\$7 .7\$\$\$\$\$7: ?\$\$\$.					
\$\$\$					
\$\$\$7\$\$\$\$\$\$\$\$\$\$\$ :\$\$\$.					
\$\$\$ \$\$\$\$\$7\$\$\$\$\$\$\$\$ .\$\$\$.					
\$\$\$ \$\$\$ 7\$\$\$7 .\$\$\$ .\$\$\$.					
\$\$\$\$ \$\$\$\$7 .\$\$\$.					
7\$\$\$7 7\$\$\$\$ 7\$\$\$					
\$\$\$\$ \$\$					
\$\$\$\$7. \$\$ (TM)					
\$\$\$\$\$\$					
\$\$\$\$\$\$\$\$\$\$7\$\$\$\$\$\$\$ . \$\$\$\$\$					
\$\$\$\$\$\$\$\$\$\$\$					
configure: Package configured for:					
configure: OS type : linux-gnu					
configure: Host CPU : x86_64					
configure: build-cpu:vendor:os: x86_64 : pc : linux-gnu	. :				
<pre>configure: host-cpu:vendor:os: x86_64 : pc : linux-gnu :</pre>					
billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$					

### Interface de sélection des modules

### (menuselect)

sudo make menuselect

contragazet nose epartenaoziost koo_ot i pe i eznak gia i
billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$ sudo make menuselect
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="silent" cmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0/menuselect »
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES -I/usr/include/libxml2 -c -o menuselect.o menuselect.c
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES   -c -o strcompat.o strcompat.c
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES -c -o menuselect_curses.o menuselect_curses.c
gcc -o cmenuselect menuselect.o strcompat.o menuselect_curses.o -lncurses -ltinfo -lxml2
make[1] : on quitte le répertoire « /usr/src/asterisk-20.13.0/menuselect »
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="silent" nmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0/menuselect »
make[1]: rien à faire pour « nmenuselect ».
make[1] : on quitte le répertoire « /usr/src/asterisk-20.13.0/menuselect »
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="silent" gmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0/menuselect »
make[1]: rien à faire pour « gmenuselect ».
make[1] : on quitte le répertoire « /usr/src/asterisk-20.13.0/menuselect »
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0 »
Generating input for menuselect

#### make :

• Outil de construction qui lit les fichiers Makefile pour automatiser le processus de compilation.

### menuselect :

- Cible spécifique du Makefile d'Asterisk.
- Construit une interface utilisateur en mode texte (TUI) permettant de sélectionner :

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 121 / 197 - CHAHROUR



- les codecs à activer,
- les modules SIP, IAX, MGCP,
- o les bibliothèques facultatives ou expérimentales,
- o et autres composants du cœur Asterisk.

### Compilation des dépendances :

- On observe la compilation de fichiers comme :
  - o menuselect.o, strcompat.o, menuselect\_curses.o
- Ces fichiers sont nécessaires au bon fonctionnement de l'interface de configuration.

### Utilisation de flags de compilation :

- -Wall : active tous les avertissements du compilateur.
- -Wno-deprecated-declarations : ignore les avertissements liés à l'usage de fonctions obsolètes.
- -DHAVE\_NCURSES, -I/usr/include/libxml2 : indique que certaines bibliothèques sont bien disponibles pour la compilation.



### Add-ons :

- Cette section regroupe les **modules supplémentaires non activés par défaut**. Ils offrent des fonctionnalités avancées ou spécifiques, non critiques pour une installation de base.
- Ces modules peuvent dépendre de bibliothèques tierces ou être destinés à des cas d'usage particuliers.
- La mention (See README-addons.txt) renvoie à un fichier inclus dans les sources Asterisk, décrivant en détail chaque module complémentaire.
- Autres sections du menu :
  - Applications : modules d'actions dans le dialplan (ex : Dial, Hangup, Voicemail).
  - **Channel Drivers** : pilotes SIP, PJSIP, DAHDI, etc.
  - Codec Translators : prise en charge des codecs audio (G.711, G.729, Opus...).
  - **PBX Modules** : fonctionnalités cœur du système PBX d'Asterisk.
  - **Sound Packages** : jeux de fichiers audio utilisés pour les annonces système ou la musique d'attente.

### Actions possibles :

- Navigation :
  - Utiliser les flèches du clavier pour se déplacer dans le menu.
  - Appuyer sur Entrée pour accéder aux sous-menus.
  - o Utiliser la touche s pour (dé)sélectionner un module.
  - Permet à l'administrateur de personnaliser finement l'installation pour ne compiler que les composants nécessaires, optimisant ainsi la performance et la sécurité de l'instance Asterisk.







### Symboles affichés :

- XXX : le module est **désactivé** et **non disponible** pour compilation, souvent en raison d'une dépendance manquante.
- [] : le module est disponible mais non sélectionné.
- [\*] : le module est sélectionné pour compilation.
- Module sélectionné :
- [\*] format\_mp3 :

### Ce module est activé pour la compilation.

- Il permet à Asterisk de lire ou d'écrire des fichiers audio au format MP3.
- Nécessite généralement la bibliothèque mp3 et l'exécution du script contrib/scripts/get\_mp3\_source.sh (comme effectué précédemment dans le processus).
- Ce module est particulièrement utile si le système doit gérer de la messagerie vocale, des musiques d'attente ou des enregistrements au format .mp3.

### Modules non activés :

- **chan\_mobile** : non compilé, dépend d'une pile Bluetooth (désactivé XXX).
- **chan\_ooh323** : désactivé par défaut, prend en charge le protocole H.323.







Après avoir modifié la configuration des modules dans **Menuselect** (comme l'activation de format\_mp3), une tentative de quitter le menu sans sauvegarder a été détectée. Menuselect interrompt alors l'action pour demander confirmation.

### Options proposées :

- Y (Yes) :
  - Quitter sans enregistrer les modifications.
  - Tout changement effectué (par exemple l'activation de modules) sera perdu.
- N (No) :
  - Annuler la sortie.
  - o Retour immédiat à l'interface Menuselect pour poursuivre la configuration.
- S (Save) :
  - Enregistrer les modifications apportées.
  - Puis quitter proprement Menuselect.
  - C'est cette option qui doit être choisie si les sélections sont définitives et prêtes à être prises en compte dans la compilation.



### DataTel

# BTSSID

### **Compilation d'Asterisk**

Cette commande compile Asterisk en utilisant tous les cœurs disponibles de ton processeur pour aller plus vite.

sudo make -j\$(nproc)

### Détail des composants de la commande :

- sudo :
  - Nécessaire pour exécuter la compilation dans un répertoire système comme /usr/src, ou pour installer ensuite les fichiers binaires dans des emplacements système.
- make :
  - Outil qui automatise le processus de compilation selon les instructions définies dans un fichier Makefile.
- -j\$(nproc) :
  - Option -j (jobs) indique le nombre de tâches (compilations) à exécuter en parallèle.
  - \$(nproc) est une substitution de commande shell renvoyant **le nombre de cœurs CPU** disponibles sur la machine.
  - Exemple : si nproc retourne 4, alors make -j4 lancera 4 processus de compilation en parallèle.
  - Cette approche permet de **réduire considérablement le temps de compilation**, en exploitant pleinement les ressources matérielles.

billy@SRV-VOIP:/usr/src/asterisk-20.13.0\$ sudo make -j\$(nproc)
 [CC] astcanary.c -> astcanary.o
 [CC] astdb2sqlite3.c -> astdb2sqlite3.o
 [CC] hash/hash.c -> hash/hash.o
 [CC] astdb2bdb.c -> astdb2bdb.o
 [CC] hash/hash\_bigkey.c -> hash/hash\_bigkey.o
 [CC] hash/hash\_buf.c -> hash/hash\_buf.o
 [CC] hash/hash\_func.c -> hash/hash\_func.o
 [CC] hash/hash\_log2.c -> hash/hash\_log2.o



### Installation des binaires + fichiers de config par défaut

sudo make install sudo make samples sudo make config sudo ldconfig

### Étapes automatiques lancées durant l'installation : sudo make samples :

- o Installe les fichiers de configuration exemples dans /etc/asterisk.
- Ces fichiers servent de base pour personnaliser le comportement d'Asterisk.
- Recommandé lors d'une première installation pour disposer d'une configuration fonctionnelle minimale.

sudo make config :

- Installe les **fichiers de service** nécessaires pour démarrer Asterisk via systemd (ou init.d selon la distribution).
- o Permet d'exécuter des commandes comme :

### sudo ldconfig :

Met à jour le cache des bibliothèques partagées du système, assurant que les bibliothèques compilées sont détectées correctement par le système au moment de l'exécution.



sudo systemctl enable asterisk Résultat :

• Le service Asterisk a bien été démarré.

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 127 / 197 - CHAHROUR





• Un message indique :

asterisk.service is not a native service, redirecting to systemd-sysv-install. Cela signifie qu'Asterisk utilise un script **SysV init** (/etc/init.d/asterisk) et non une unité native systemd.  $\rightarrow$ Ce comportement est **normal et attendu** sur certaines installations manuelles ou personnalisées.

```
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo systemctl start asterisk
sudo systemctl enable asterisk
asterisk.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable asterisk
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Vérifie que tout fonctionne :

sudo systemctl status asterisk

Service actif et en cours d'exécution :

```
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo systemctl status asterisk

• asterisk.service - LSB: Asterisk PBX

Loaded: loaded (/etc/init.d/asterisk; generated)

Active: active (running) since Sun 2025-04-20 20:12:36 CEST; 56s ago

Docs: man:systemd-sysv-generator(8)

Tasks: 66 (limit: 2273)

Memory: 43.3M

CPU: 3.016s

CGroup: /system.slice/asterisk.service

L34828 /usr/sbin/asterisk

avril 20 20:12:36 SRV-VOIP systemd[1]: Starting asterisk.service - LSB: Asterisk PBX...

avril 20 20:12:36 SRV-VOIP asterisk[34816]: Starting Asterisk PBX: asterisk.

avril 20 20:12:36 SRV-VOIP systemd[1]: Started asterisk.service - LSB: Asterisk PBX.

billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Le service Asterisk est démarré avec succès, tourne actuellement, et a bien été activé pour démarrage automatique au prochain boot.

### **Configuration SIP avec PJSIP**

Éditer le fichier pjsip.conf pour ajouter les comptes utilisateurs SIP

sudo nano /etc/asterisk/pjsip.conf

Ce fichier constitue un **guide de référence rapide** pour la configuration du module **PJSIP** dans Asterisk. Il ne remplace pas une documentation complète mais fournit :

- Des exemples de configuration minimale, utiles comme point de départ.
- Une **liste condensée des options de configuration** extraites depuis les fichiers XML de configuration.

**Important** : Le fichier **ne contient pas** la documentation exhaustive de toutes les options possibles. Il est recommandé de se référer à la documentation officielle pour des configurations complexes ou spécifiques.







- protocol=udp : Utilise le protocole UDP pour les communications SIP.
- **bind=0.0.0.0** : Écoute sur toutes les interfaces réseau disponibles.

### Utilisateur Alice (poste 1001)



définie ci-dessous. aors=alice : Associe le point de contact (AOR).

Auth – [alice-auth]

### Endpoint – [alice]

**type=endpoint** : Déclare un terminal SIP (ici, Alice). **transport=transport-udp** : Associe le transport défini plus haut.

**context=from-internal** : Définit le contexte du dialplan utilisé pour cet utilisateur.

disallow=all / allow=ulaw : Bloque tous les codecs sauf ulaw. auth=alice-auth : Associe la section d'authentification



type=auth : Déclare une méthode d'authentification. auth\_type=userpass : Authentification par nom d'utilisateur / mot de passe. username / password : Identifiants SIP de connexion.



#### AOR – [alice]



simultanément.

type=aor : Déclare un "Address Of Record", qui gère l'enregistrement de l'utilisateur. max\_contacts=1 : Autorise un seul contact enregistré







#### Utilisateur Bob (poste 1002)

Même structure que pour Alice, dupliquée avec ses propres identifiants.

; === UTILISATEUR BOB (1002) ===
[bob]
type=endpoint
transport=transport-udp
context=from-internal
disallow=all
allow=ulaw
auth=bob-auth
aors=bob
na ann

type=aor max\_contacts=1

Les mots de passe utilisés dans cet exemple sont simples à des fins pédagogiques.

En production, il est impératif d'utiliser des mots de passe complexes pour éviter toute compromission SIP.

### Éditer le fichier extensions.conf

sudo nano /etc/asterisk/extensions.conf

Ce fichier est le cœur du comportement d'appel dans Asterisk. Il permet de définir :



 les règles de traitement des appels entrants et sortants.

 les actions à exécuter selon les numéros composés,

• l'utilisation de contextes pour segmenter les droits et flux.

Descendre jusqu'en bas du fichier

Cette section est un **contexte logique du plan de** 

numérotation (dialplan) dans Asterisk.

Elle est utilisée pour diriger les appels internes des utilisateurs SIP déclarés (ex. alice et bob).

[from-internal] exten => 1001,1,Dial(PJSIP/alice,20) exten => 1002,1,Dial(PJSIP/bob,20)

exten => 1001,1,Dial(PJSIP/alice,20) •

Epreuve E6 – Situation professionnelle 2 - Documentation Technique - Page 131 / 197 - CHAHROUR



- **1001** : Numéro d'extension que l'utilisateur peut composer.
- 1 : Priorité d'exécution dans le dialplan.
- Dial(PJSIP/alice,20) :
  - Demande à Asterisk de joindre l'utilisateur alice via le canal PJSIP.
  - La sonnerie durera 20 secondes maximum avant d'échouer ou de passer à une priorité suivante (si définie).
- exten => 1002,1,Dial(PJSIP/bob,20)
- Fonctionnement identique, mais pour l'utilisateur bob.
- Lorsqu'un utilisateur compose 1001, l'appel sera redirigé vers le terminal Alice.
- Lorsqu'un utilisateur compose 1002, l'appel sera redirigé vers le terminal Bob.
- Ce contexte doit être référencé dans chaque endpoint SIP comme suit :

context=from-internal



### **Recharger les fichiers depuis la console CLI Asterisk**

Accède à la console :

sudo asterisk -rvvv

sudo : Nécessaire pour accéder au processus Asterisk avec les privilèges adéquats.

**asterisk** : Lance le client d'Asterisk.

-r : Se connecte à une instance Asterisk déjà en cours d'exécution (mode *remote console*).

-vvv : Définit le niveau de verbosité à 3, permettant d'obtenir un retour détaillé sur les événements en temps réel (enregistrement, appels, erreurs, etc.).



La connexion au service Asterisk a réussi.

L'instance tourne sous la version **20.13.0**.

Le processus principal Asterisk a pour PID **34828**.

Le prompt interactif SRV-VOIP\*CLI> indique que la **console CLI d'Asterisk est accessible**, prête à recevoir des commandes comme :

cette commande permet de **recharger dynamiquement les modules PJSIP** à partir des fichiers de configuration (pjsip.conf, etc.) **sans redémarrer Asterisk**.

Modules rechargés avec succès :

- res\_pjsip.so : composant principal du moteur SIP PJSIP.
- res\_pjsip\_authenticator\_digest.so : gestion de l'authentification digest SIP.
- res\_pjsip\_endpoint\_identifier\_ip.so : identification des endpoints par adresse IP.
- res\_pjsip\_mwi.so : gestion des notifications de message en attente (MWI).



- res\_pjsip\_notify.so : support pour les messages NOTIFY SIP.
- res\_pjsip\_outbound\_publish.so : publication d'événements SIP.
- res\_pjsip\_publish\_asterisk.so : publication des événements internes Asterisk.
- res\_pjsip\_outbound\_registration.so : enregistrement SIP vers des serveurs externes



Ceci n'est pas une erreur mais une **notification informative**. Certains objets internes (system) ne peuvent pas être rechargés dynamiquement ; les anciennes valeurs sont donc conservées.

### Commande 2 : dialplan reload

Recharge le fichier /etc/asterisk/extensions.conf et toute autre source de plan de numérotation.

### Confirmation affichée :



- Variables globales définies :
  - CONSOLE  $\rightarrow$  Console/dsp
  - TRUNK → DAHDI/G2
  - $\circ$  TRUNKMSD  $\rightarrow$  1

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 134 / 197 - CHAHROUR



### • Switches inclus :

- DUNDI/e164 et ael-dundi-e164-switch :
  - Ces entrées indiquent que des composants AEL (Asterisk Extension Language) ou DUNDi (Distributed Universal Number Discovery) sont présents ou référencés.

Les commandes de rechargement ont été exécutées avec succès, ce qui confirme que :

- Les modifications des fichiers pjsip.conf et extensions.conf ont bien été prises en compte.
- Le système est prêt à traiter les appels selon la configuration en place.

## Étape 1 – Télécharger Zoiper 5

- 1. Ouvrir un navigateur web.
- 2. Accéder au site officiel de Zoiper à l'adresse suivante : https://www.zoiper.com/en/voip-softphone/download/current
- 3. Cliquer sur **"Download"** sous la version correspondant à votre système d'exploitation :
  - o Windows
  - o macOS
  - o Linux
  - Mobile (Android / iOS)

### Étape 2 – Installer Zoiper

### Pour Windows :

- 1. Exécuter le fichier téléchargé (Zoiper5\_Installer.exe).
- 2. Accepter les conditions d'utilisation.
- 3. Cliquer sur "Next" jusqu'à la fin de l'installation.
- 4. Une fois installé, lancer Zoiper 5.



# Étape 3 – Lancer Zoiper (Community Edition)

Après avoir validé les identifiants et la connexion, Zoiper vous propose de choisir entre la version gratuite (Community Edition) et la version payante (PRO).

### Édition Community Edition détectée

Le message vous informe que vous utilisez **Zoiper5 Community Edition**, qui est **gratuite** pour une utilisation non commerciale. Cette version permet les appels VoIP de base avec les fonctionnalités essentielles.

### Choisir l'option gratuite

Pour continuer avec la version gratuite, cliquez simplement sur le lien **"Continue as a Free user"**. Cette action permet d'utiliser Zoiper sans licence payante tout en conservant les fonctionnalités de base nécessaires pour s'enregistrer et passer des appels.



Cliquez sur "Continue as a Free user".





Après avoir défini l'adresse du serveur VoIP, l'utilisateur est invité à **renseigner ses identifiants de connexion SIP** afin de s'enregistrer auprès du serveur.

### □Champ "Username / Login"

Il faut saisir ici **le nom d'utilisateur SIP** attribué. Ce nom est généralement fourni par l'administrateur système ou configuré sur le serveur VoIP (par exemple : 101, alice, techsupport, etc.).

### Champ "Password"

Dans ce champ, saisir **le mot de passe associé** au compte SIP utilisé. Ce mot de passe est requis pour permettre l'authentification sécurisée de l'utilisateur auprès du serveur.

### Connexion

Une fois les deux champs correctement remplis, cliquer sur **"Login"** pour tenter une connexion au serveur VoIP.

Si les identifiants sont valides, l'enregistrement SIP sera effectué et l'utilisateur pourra ensuite émettre et recevoir des appels.

En cas d'échec, vérifier l'exactitude des informations saisies ainsi que la configuration du compte côté serveur.



Lors de cette étape, il est nécessaire de spécifier l'adresse du serveur SIP auquel le client Zoiper devra se connecter pour établir la communication VoIP.

### Champ Hostname

Dans le champ "Hostname", il convient de renseigner **l'adresse IP de la machine hébergeant le serveur VoIP** (généralement Asterisk, FreePBX ou équivalent).





Dans cet exemple, l'adresse renseignée est : 192.168.10.60 Cette adresse correspond à la **machine serveur VoIP située sur le réseau local**. Elle peut aussi être un nom de domaine si le serveur est accessible via Internet (ex. voip.entreprise.fr).



Après avoir saisi correctement l'adresse IP ou le nom de domaine, cliquer sur le bouton **Next** pour valider cette configuration et passer à l'étape suivante de l'assistant. Remarque : Veillez à ce que le poste

client ait un accès réseau direct à cette adresse IP, et que les ports SIP (ex : 5060 pour UDP) soient ouverts sur le serveur.

À ce stade, Zoiper propose de configurer des paramètres supplémentaires liés à l'authentification avancée et à l'utilisation d'un **proxy SIP sortant**.

### Authentication username

Ce champ permet de spécifier un nom d'utilisateur différent pour l'authentification, dans le cas où celuici ne correspond pas exactement au nom de compte SIP utilisé pour l'enregistrement. Exemple d'usage : lorsque le login est différent de l'extension SIP (cas rare dans un environnement standard).

### Outbound proxy

Ce champ est destiné aux infrastructures où un **proxy SIP** est nécessaire pour le routage des paquets VoIP, notamment dans des environnements réseau complexes ou avec inspection approfondie (firewall/proxy d'entreprise).

### Choix recommandé :

Dans le cadre d'un déploiement simple ou classique (comme avec un serveur Asterisk local ou distant sans proxy spécifique), **aucun paramètre supplémentaire n'est requis** à cette étape.





Il convient donc de cliquer (bouton en bas à gauche) ignorer cette configuration à l'étape suivante.



sur **Skip** pour et passer

À cette étape de la configuration, **Zoiper5** teste automatiquement les types de transport disponibles pour établir une connexion avec le serveur SIP. Il s'agit d'une phase essentielle permettant de garantir la compatibilité entre le client (Zoiper) et le serveur VoIP (ex. : Asterisk, FreePBX, etc.).

Résultat du test :

• SIP UDP : Found

 $\rightarrow$  Le protocole SIP en UDP a été détecté avec succès. C'est le mode de transport le plus couramment utilisé dans les environnements VoIP classiques car il est léger et efficace pour les communications en temps réel.

• SIP TCP : Not found

 $\rightarrow$  Le protocole SIP en TCP n'a pas été détecté. Cela signifie que le serveur ne prend pas en charge ce mode, ou que le port correspondant n'est pas accessible.

• SIP TLS : PRO (non disponible dans la version gratuite)

 $\rightarrow$  Le protocole chiffré SIP TLS est réservé à la version professionnelle de Zoiper.

• IAX UDP : Not found

 $\rightarrow$  Le protocole IAX n'a pas été détecté. Il est moins utilisé mais parfois préféré pour les communications inter-Asterisk.

### Action recommandée :

Sélectionner **SIP UDP** (qui est déjà mis en surbrillance en vert) et cliquer sur **Next** pour poursuivre la configuration.

C'est le protocole recommandé dans la majorité des cas, sauf environnement spécifique avec exigences de sécurité élevées (où SIP TLS serait utilisé).

### DataTel

# BTSSID



l'interface principale de **Zoiper** permet de valider que l'utilisateur est bien enregistré sur le serveur VoIP.



1 Confirmation de l'enregistrement

• En haut à gauche, la mention **alice@192.168.10.60** indique que l'utilisateur **Alice** est connecté avec succès au serveur SIP situé à l'adresse IP **192.168.10.60**.

• La présence de la **coche verte** confirme l'état « **connecté** » (enregistré avec succès auprès du serveur IPBX/Asterisk).

### 2Accès à l'interface d'appel

• Le bouton représentant un **clavier téléphonique** permet d'ouvrir le **pavé numérique** afin de composer un numéro ou un identifiant SIP pour passer un appel.

À ce stade, l'utilisateur est prêt à émettre ou recevoir des appels via le système VoIP.





### Étapes de configuration et de test

- 1. Connexion des deux utilisateurs :
  - Les deux utilisateurs ont été connectés à l'aide de leur identifiant SIP fourni par le serveur IPBX.
  - La capture montre que l'utilisateur alice est bien authentifié sur le serveur VOIP à l'adresse IP 192.168.10.60, ce qui est confirmé par la coche verte à côté de son identifiant : <u>alice@192.168.10.60</u>.



- 2. Composition du numéro :
  - Dans l'interface de Zoiper, l'utilisateur a accédé au pavé numérique via l'icône du clavier (visible dans la barre supérieure).
  - Le numéro ou l'identifiant SIP de l'utilisateur à contacter (**bob**) a été saisi, puis l'appel a été initié en cliquant sur **Dial** (composer).
- 3. Établissement de l'appel :





- Une fois l'appel lancé, la fenêtre d'appel s'affiche avec les informations de contact de **bob**, telles que son identifiant SIP, l'état de la connexion (barres de signal), et la durée de l'appel.
- L'appel est actif comme l'indique le compteur de durée (ici 00:02 secondes).
- 4. Réception de l'appel par le correspondant :

🥩 Zoiper5	- 🗆 X
✓ bob@192.168.10.60 🔅	
Q Find a contact	$ \begin{array}{c c c c c c c c c c c c c c c c c c c $
Calls	wite speake keypati statisats kecord video from fransier Adultan
1001 bob@192.168.10.60 00:02	Ringing
Contacts Recent	1001
All Calls Messages	1001 bob@192.168.10.60 0002
1001 2 1001 9:40 PM	
	e •

- L'utilisateur **bob** reçoit un appel entrant provenant de **alice**.
- o Zoiper affiche la fenêtre de notification de l'appel entrant avec trois options :
  - Accepter
  - X Refuser
  - Iransférer
- 5. Communication active :
  - Une fois l'appel accepté, les deux utilisateurs sont en communication bidirectionnelle.
  - Les boutons de gestion d'appel (mute, haut-parleur, statistiques, transfert, etc.) deviennent accessibles pour ajuster la session selon les besoins.

### < Résultat du test

Le test est concluant. La communication entre les deux utilisateurs **alice** et **bob** a bien été établie via le protocole **SIP UDP**, qui a été validé lors de la phase de détection des services VoIP disponibles. Cela confirme que :

• Le serveur IPBX est opérationnel,



- Les comptes SIP sont fonctionnels et correctement configurés,
- Les flux réseau ne sont pas bloqués par un pare-feu,
- L'environnement réseau autorise bien le transport UDP sur les ports SIP.

### **Annexe – Définitions des termes techniques**

### 1. VM (Virtual Machine)

Machine virtuelle qui simule un ordinateur physique dans un environnement logiciel, permettant de tester ou déployer des systèmes indépendamment du matériel réel.

### VMware

Logiciel de virtualisation qui permet de créer et gérer des machines virtuelles.

### Bridge (mode réseau)

Mode de connexion réseau dans VMware où la machine virtuelle est connectée comme un poste du réseau local.

### Debian

Distribution GNU/Linux stable et utilisée en environnement serveur, ici version 12 (Bookworm). **SRV-VOIP** 

Nom d'hôte attribué au serveur dédié à la téléphonie VoIP avec Asterisk.

### Adresse IP

Identifiant unique d'un appareil sur un réseau (exemple : 192.168.10.60).

### Masque de sous-réseau

Paramètre qui détermine la taille d'un réseau local (ex : 255.255.255.0 = /24).

### Passerelle (Gateway)

Routeur qui permet à une machine de communiquer avec des réseaux extérieurs, comme Internet.

### DNS (Domain Name System)

Système de résolution de noms permettant de traduire un nom (ex. google.com) en adresse IP.

### APT

Gestionnaire de paquets utilisé dans Debian pour installer, mettre à jour ou supprimer des logiciels. **Sudo** 

Commande permettant d'exécuter une action en tant qu'administrateur (root).

### Root

Compte administrateur principal sous Linux, ayant tous les droits.

### Utilisateur standard

Compte utilisateur limité, utilisé pour les tâches courantes, sans accès complet au système.

### Partition

Partie d'un disque dur utilisée pour organiser les données (ex : partition système, swap...).

### Swap

Zone du disque utilisée comme mémoire virtuelle quand la RAM est saturée.

### GRUB

Chargeur de démarrage qui permet de lancer le système d'exploitation installé.

### Terminal (console TTY)

Interface en ligne de commande permettant d'interagir avec le système via du texte.

### Make / Makefile

Outil et fichier permettant d'automatiser la compilation d'un logiciel.



### wget / curl

Commandes permettant de télécharger des fichiers depuis Internet via ligne de commande.

### build-essential

Paquet contenant les outils de base pour compiler des logiciels (gcc, make, etc.).

### lib...-dev

Bibliothèques de développement nécessaires à la compilation de logiciels (ex. : libxml2-dev).

### pkg-config

Outil pour obtenir des informations de compilation sur les bibliothèques installées.

### tar.gz

Archive compressée contenant souvent des fichiers sources à extraire avant compilation.

### Asterisk & VoIP

### Asterisk

Logiciel libre de téléphonie IP (PBX), permettant de gérer appels, messagerie vocale, conférences, etc. VoIP (Voice over IP)

Technologie permettant de passer des appels téléphoniques via Internet ou réseau IP.

### IPBX

Standard téléphonique IP, souvent basé sur Asterisk, qui gère les appels internes et externes.

### SIP (Session Initiation Protocol)

Protocole réseau utilisé pour établir, modifier et terminer des appels VoIP.

### PJSIP

Nouvelle implémentation du protocole SIP intégrée dans Asterisk, plus performante et modulaire.

### pjsip.conf

Fichier de configuration d'Asterisk pour les utilisateurs SIP avec PJSIP.

### extensions.conf

Fichier de configuration du plan de numérotation (dialplan) d'Asterisk.

### Endpoint

Équipement ou logiciel (comme Zoiper) qui se connecte à Asterisk pour passer/recevoir des appels.

### AOR (Address of Record)

Point de contact SIP permettant de localiser un utilisateur dans un réseau VoIP.

### Auth

Section du fichier PJSIP définissant le mode d'authentification d'un utilisateur SIP.

### Context

Groupe logique de règles dans le dialplan, associé à un ou plusieurs endpoints.

### Dialplan

Ensemble de règles définissant comment les appels sont traités et routés dans Asterisk.


## Zoiper

Client SIP (softphone) permettant de passer des appels via un ordinateur ou smartphone. **Softphone** 

Logiciel qui simule un téléphone, utilisé pour la téléphonie sur IP.

## SIP UDP / TCP / TLS

Méthodes de transport du protocole SIP :

- UDP : rapide, non sécurisé (le plus courant),
- TCP : plus fiable mais moins courant,
- TLS : sécurisé (crypté), réservé aux versions pro de Zoiper.

### **Outbound Proxy**

Serveur intermédiaire qui achemine les messages SIP, utilisé dans des réseaux complexes.

### Authentication Username

Identifiant utilisé pour s'enregistrer auprès du serveur SIP.





# Création, d'une VM sur VM WARE

Lorsque vous créer une machine virtuelle l'option « Typical (recommended) est cocher de base.



Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 146 / 197 - CHAHROUR Walid





Dans notre cas à nous allons choisir « Linux » car nous auront besoin d'installer d'un pare-feu sur le serveur

	New Virtual Machine Wizard	×
Cliquer dans le menu déroulant puis sélectionner « Linux»	Select a Guest Operating System Which operating system will be installed on this virtual machine	?
Cliquer sur « Next » pour passer à la prochaine étape	Guest operating system OMicrosoft andows OMicrosoft and ows OMicrosoft	
Dans cette étape nous allons devoir nommer le serveur ainsi que choisir		
New Virtual Machine Wizard		
Name the Virtual Machine What name would you like to use for this virtual machine	e Help < <u>B</u> ack <u>Next</u> >	Can 3
Virtual machine name: RTE-01	l'emplacement de la VM	
Location:	(1) Ensuite nous allons nommer	<sup>-</sup> le server
SRV-E-brigade	(2) Choisir l'emplacement ou se	era situé la VM
SRV-E-brigade	(3) Cliquer sur « Next » pour pa prochaine étape	sser à la
< Back Next >		

Ensuite sur cette étape nous allons allouer

l'espace du disque pour notre serveur. Dans notre cas il n'est pas nécessaire d'avoir un gros espace de stockage sur notre serveur.





Cliquer sur « Next » pour passer à la prochaine étape	New Virtual Machine Specify Disk Capa How large do yo	Nizard ×	
	The virtual machine's ha physical disk. These file( files, and data to your v Maximum disk size (GB):	rd disk is stored as one or more files on the host computer's s) start small and become larger as you add applications, irtual machine.	
	Recommended size for L	lbuntu: 20 GB	
	<ul> <li>Store virtual disk as a</li> <li>Split virtual disk into i</li> <li>Splitting the disk makes</li> <li>but may reduce performed</li> </ul>	a single file <u>m</u> ultiple files tes it easier to move the virtual machine to another computer formance with very large disks.	
Ensuite dans cette partie-là nous configurer les options suivantes :			allons
New Virtual Machine Wizard	×		
Ready to Create Virtual Machine Click Finish to create the virtual machine. Then you c	an install Ubuntu.	<u>Back</u> <u>Next</u> Cancel Cliquer sur « Customize Hardware »	
The virtual machine will be created with the following settin	gs:		
Name:     RTE-01       Location:     E:\VM\BTS-SIO\AP4\RTE-01       Version:     Workstation 17.5 or later       Operating System:     Ubuntu			
Hard Disk:     20 GB, Split       Memory:     4096 MB       Network Adapter:     NAT       Other Devices:     2 CPU cores, CD/DVD, USB Controlled	r, Sound Card		
<u>Qustomize Hardware</u>			
		Dans cette partis nous allons paramétro	er selon
< <u>B</u> ack Fir	nish Cancel	nos desoins :	





(2) 14	Hardware		×	
<ul> <li>(10)CD/ DVD = Pfsens</li> <li>(11)Network Adapter = Vmnet 4 Network Adapter = Vmnet 4</li> <li>Network adapter = Vmnet 1</li> <li>(12)Cliquer sur « Close » pour fenêtre</li> </ul>	Device     Summary       ■ Processors     2       ● Network Adapter     Custom (VMnet4)       ▷ Network Adapter     Custom (VMnet4)       ▷ Network Adapter     Custom (VMnet4)       ○ Sound Card     Auto detect       □ Displey     Auto detect	Memory Specify the amount: size must be a multipression of this with list of the second second second second second size must be a multiple size must be a multiple size m	of memory allocated to this virtual machine. The memory ple of 4 MB. ual machine: 4096 WB Maximum recommended memory (Memory swapping may occur beyond this size.) 27.9 GB Recommended memory 4 GB Guest OS recommended minimum 2 GB	(bridge) (bridge) fermer la
Une fois que la configuration vous aller avoir ce menu-là : New Virtual Machine Wizard <b>Ready to Create Virtual Machine</b> Click Finish to create the virtual m	Add Remove	×	(Close Help	est finit
The virtual machine will be created with Name: RTE-01 Location: E:\VM\BTS-SIO\AR Version: Workstation 17.5 Operating System: Ubuntu Hard Disk: 20 GB, Split Memory: 4096 MB Network Adapter: Custom (VMnet4), Other Devices: 2 CPU cores, CD/T Customize Hardware	the following settings: 24\RTE-01 or later 0 Custom (VMnet4), Custom (VMnet1) DVD, USB Controller, Sound Card	(5 du (6 la	5) Récapitulatif de la con u serveur. 5) Cliquer sur « Finish » p i prochaine étape	figuration bour passer à
	Finish Canc	U in Vi el vo	Ine fois avoir fini de vérific nformation du serveur, la irtual Machine) va se crée ous pouvez le lancer.	er les VM ( er ainsi

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 149 / 197 - CHAHROUR Walid









# **Installation Ubuntu Server 22.04**

Lors du démarrer vous aurez un message avec plusieurs choix possible :



Sélectionner Terminé

















### Sélectionner Terminé

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 154 / 197 - CHAHROUR Walid







Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 155 / 197 - CHAHROUR Walid





Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 156 / 197 - CHAHROUR Walid





Ubuntu 24.04.2 LTS srv-e-brigade tty1

srv-e-brigade login:



# Fixer une IP sur Ubuntu

Donc lorsque la machine vient de booter sur l'os Ubuntu nous allons fixer l'IP via cette commande : sudo nano /etc/netplan/00-installer-config.yaml



BTSSID

Une fois après avoir quitter le fichier de conf taper les commande suivantes

sudo netplan apply

### sudo chmod 600 /etc/netplan/00-installer-config.yaml

- (1) Problème de droit donc taper la commande avec sudo chmod
- (2) Puis appliquer la configuration

Une fois fait vérifier si l'ip c'est bien

en statique via la commande suivante :

(generate:1636): others.	WARNING	же: 2	L:49:43.	010:	Permiss	ions fo	r ∕eto	:/netpla	an/00-	install	er-conf	ig.yaml	l are	too	open.	Netplar	conf:	guratio	n shou]	d NOT	be	accessible
(process:1634): others.	WARNING				ermissi			'netplar				g.yaml				Netplan	config				be a	
(process:1634):	WARNING	www. 21		56: P	ermissi	ons for	/etc/	netplar	n/00-1	installe	-confi	g.yaml	are	too d	open.	Netplan	conflg	uration	should	NOT	be a	ccessible
otners. ly@srv-e-brigade ly@srv-e-brigade ly@srv-e-brigade	: **\$ sudo : **\$ sudo : **\$	chmod netpla	600 ∕et an apply	c/net	plan/00	-instal	ler-co	onfig.ya	aml	2												



Pour finir nous allons vérifier si le serveur E-brigade est bien connecter au réseau via les commande suivantes :





### Ping 8.8.8.8 Ping YouTube .com

billy@srv-e-brigade:~\$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp\_seq=1 ttl=115 time=10.4 ms
64 bytes from 8.8.8.8: icmp\_seq=2 ttl=115 time=10.5 ms
64 bytes from 8.8.8.8: icmp\_seq=3 ttl=115 time=10.1 ms
64 bytes from 8.8.8.8: icmp\_seq=4 ttl=115 time=10.3 ms
^C
--- 8.8.8.8 ping statistics --4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 10.111/10.349/10.533/0.154 ms
billy@srv-e-brigade:~\$ ping youtube.com
PING youtube.com (142.250.75.238) 56(84) bytes of data.
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp\_seq=1 ttl=115 time=10.7 ms
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp\_seq=2 ttl=115 time=10.8 ms
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp\_seq=3 ttl=115 time=10.6 ms
^C
--- youtube.com ping statistics --3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 10.590/10.704/10.775/0.081 ms
billy@srv-e-brigade:~\$

Comme vous pouvez le constater le ping fonctionne bien avec l'ip ou le nom de domaine .



# **Installation e- brigade**

BTSSID

Avant de réaliser l'installation assurer-vous que votre Ubuntu soit bien à jour via cette commande

### sudo apt update && sudo apt upgrade -y

a maintenance de sécurité étendue pour Applications n'est pas activée.

jour peut être appliquée immédiatement.

tivez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires. sitez https://ubuntu.com/esm ou executez : sudo pro status

ailed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

sudo apt upgrade -v

billy@srv-e-brigade:~\$ sudo apt update && sudo apt upgrade -v
[sudo] password for billy:
Atteint :1 http://archive.ubuntu.com/ubuntu noble InRelease
Réception de :2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Réception de :3 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Réception de :4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Réception de :5 http://archive.ubuntu.com/ubuntu noble/main Translation-fr [491 kB]
Réception de :6 http://archive.ubuntu.com/ubuntu noble/main amd64 c-n-f Metadata [30,5 kB]
Réception de :7 http://archive.ubuntu.com/ubuntu noble/restricted Translation-fr [3 292 B]
Réception de :8 http://archive.ubuntu.com/ubuntu noble/restricted amd64 c-n-f Metadata [416 B]
Réception de :9 http://archive.ubuntu.com/ubuntu noble/universe Translation-fr [3 898 kB]
Réception de :10 http://archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Réception de :11 http://archive.ubuntu.com/ubuntu noble/multiverse Translation-fr [89,0 kB]
Réception de :12 http://archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8 328 B]
Réception de :13 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [979 kB]
Réception de :14 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [215 kB]
Réception de :15 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Réception de :16 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [13,5 kB]
Réception de :17 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [876 kB]
Réception de :18 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [177 kB]
Réception de :19 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Réception de :20 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [492 B]
Réception de :21 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1 046 kB]
Réception de :22 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [263 kB]
Réception de :23 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [365 kB]
Réception de :24 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [26,0 kB]
Réception de :25 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [21,5 kB]
Réception de :26 http://archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [4 788 B]
Réception de :27 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Réception de :28 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [592 B]
0% [18 Translation-en store 0 B] [Attente des fichiers d'en-tête]

Taper le mot de passe

Une fois après avoir réaliser la mise à jour nous allons installer maria db via cette commande :

### sudo apt install mariadb-server -y



### sudo mysql\_secure\_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current password for the root user. If you've just installed MariaDB, and haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):

illy@srv-e-brigade:~\$ sudo mysql\_secure\_installation

Entrer un mot de passe



répondre



Change the root password? [Y/n] n ... skipping. By default, a MariaDB installation has an anonymous user, allowing anyone to log into MariaDB without having to have a user account created for Voici ce que vous devez This is intended only for testing, and to make the installation them. go a bit smoother. You should remove them before moving into a production environment. Remove anonymous users? [Y/n] y ... Success! Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network. Disallow root login remotely? [Y/n] y ... Success! By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment. Remove test database and access to it? [Y/n] y - Dropping test database... ... Success! Création - Removing privileges on test database... ... Success! de la base Reloading the privilege tables will ensure that all changes made so far will take effect immediately. de données Reload privilege tables now? [Y/n] y ... Success! Cleaning up... e-bigade

Pour cela nous allons créer la base via cette commande :

sudo mysql -u root CREATE DATABASE ebrigade\_db; CREATE USER 'billy'@'localhost' IDENTIFIED BY 'Testap04@'; GRANT ALL PRIVILEGES ON ebrigade\_db.\* TO 'billy'@'localhost';

billy@srv-e-brigade:~\$ sudo mysql -u : Welcome to the MariaDB monitor. Comm Your MariaDB connection id is 39 Server version: 10.11.11-MariaDB-0ubu	root ands end with ; or \g. ntu0.24.04.2 Ubuntu 24.04	Comme vous pouvez le voir
Copyright (c) 2000, 2018, Oracle, Mar	iaDB Corporation Ab and others.	les commandes ont était
Type 'help;' or '\h' for help. Type '	<pre>\c' to clear the current input statement.</pre>	prise en compte
<pre>MariaDB [(none)]&gt; CREATE DATABASE ebr: Query OK, 1 row affected (0,005 sec)</pre>	igade_db;	
MariaDB [(none)]> CREATE USER 'billy' N ebrigade_db.* TO 'billy'@'localhost Query OK, 0 rows affected (0,016 sec)	@'localhost' IDENTIFIED BY 'Testap04@'; ';	FLUSH PRIVILEGES;
MariaDB [(none)]> GRANT ALL PRIVILEGE Query OK, 0 rows affected (0,005 sec)	S ON ebrigade_db.* TO 'billy'@'localhost';	EXIT;
MariaDB [(none)]>	MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebr Query OK, 0 rows affected (0,005 sec)	rigade_db.* TO 'billy'@'localhost';
Comme vous pouvez le voir les commandes ont était prise en	MariaDB [(none)]> FLUSH PRIVILEGES; Query OK, 0 rows affected (0,005 sec)	
compte	MariaDB [(none)]> EXIT; Bye billy@srv-e-brigade:~\$	

Epreuve E6 – Situation professionnelle 2 - Documentation Technique - Page 161 / 197 - CHAHROUR



# **Installation Apache 2**

Dans cette partie nous allons installer apache 2 via cette commande :

sudo apt install apache2 -y

billy@srv-e-brigade:~\$ sudo apt install apache2 -y Lecture des listes de paquets… 77%

# Une fois avoir installer nous allons télécharger les indépendances via cette commandes :

sudo apt install software-properties-common -y

sudo add-apt-repository ppa:ondrej/php -y

sudo apt update

\*\*\* Le système doit être redémarré \*\*\* Last login: Tue Apr 1 09:12:27 2025 from 192.168.20.1 billy@srv-e-brigade:~\$ sudo apt install software-properties-common -y sudo add-apt-repository ppa:ondrej/php -y sudo apt update [sudo] password for billy: Lecture des listes de paquets… 99%

billy@srv-e-brigade:~\$ sudo systemctl restart apache2

Puis nous allons installer PHP 7.4 +

extension via cette commande :

sudo apt install php7.4 libapache2-mod-php7.4 php7.4-mysql php7.4-xml php7.4-gd php7.4-curl -y



commande :

sudo systemctl restart apache2

**billy@srv-e-brigade:~\$** Une fois gue PHP est

installer nous allons vérifier la version via cette commande :

php -v



Version sur 7.3 ou plus

# Téléchargement de l'archive depuis la source officielle

Une fois que la bonne version de PHP est installé nous allons extraire le fichier via cette commande :

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 162 / 197 - CHAHROUR Walid



cd ~ wget https://ciscoursegoules.fr/wp-content/uploads/2022/08/ebrigade-5.3.2.zip unzip ebrigade-

<pre>silly@srw-e-brigade:-\$ cd ~ mget https://ciscoursegoules.fr/wp-content/uploads/2022/08/ebrigade-5.3.2.zip unzip ebrigade-5.3.2.zip 2025-04-01 11:44:14 https://ciscoursegoules.fr/wp-content/uploads/2022/08/ebrigade-5.3.2.zip Resolving ciscoursegoules.fr (ciscoursegoules.fr) 217.160.0.168, 2001:8d8:100f:f000::2cd Connecting to ciscoursegoules.fr (ciscoursegoules.fr)[217.160.0.168]:443 connected. Length: 3d4675926 (33M) [application/zip] Saving to: 'ebrigade-5.3.2.zip'</pre>				
ebrigade-5.3.2.zip 74%[====================================	24,64M	5,24MB/s	eta 4s	

Une fois après avoir télécharger l'archive le serveur va vous demander d'installer unzip dans le cas ou votre machine na pas le logiciel

Taper le mot de passe sudo

BTSSID

billy@srv-e-brigade:~\$ sudo apt install unzip [sudo] password for billy: Lecture des listes de paquets... Fait Construction de l'arbre des dépendances... Fait Lecture des informations d'état... Fait

passe ainsi avoir

Après avoir taper le mot de extrai le fichier via cette commande :

unzip ebrigade-5.3.2.zip

pilly@srv-e-brigade:~\$ unzip ebrigade-5.3.2.zip Archive: ebrigade-5.3.2.zip inflating: ebrigade-5.3.2/.gitattributes inflating: ebrigade-5.3.2/.gitignore inflating: ebrigade-5.3.2/.htaccess.template inflating: ebrigade-5.3.2/.about.php

Une fois faits-nous allons copier le repertoire web via

cette commande :

### sudo cp -r ~/ebrigade-5.3.2 /var/www/html/ebrigade

billy@srv-e-brigade:~\$ sudo cp -r ~/ebrigade-5.3.2 /var/www/html/ebrigade billy@srv-e-brigade:~\$ |

Après avoir copier nous allons attribuer les permission via ces commandes :

sudo chown -R www-data:www-data /var/www/html/ebrigade

sudo chmod -R 755 /var/www/html/ebrigade

billy@srv-e-brigade:~\$ sudo chown -R www-data:www-data /var/www/html/ebrigade sudo chmod -R 755 /var/www/html/ebrigade billy@srv-e-brigade:~\$

# **Configuration Apache pour E-brigade**

Pour cela nous allons créer un fichier de configuration via cette commande :

### sudo nano /etc/apache2/sites-available/ebrigade.conf

Une fois avoir rentrer ces information là faite ctr + x puis appuyer sur entrer pour valider <VirtualHost \*:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/ebrigade
ServerName 192.168.20.11
<Directory /var/www/html/ebrigade>
Options Indexes FollowSymLinks
AllowOverride All
Require all granted
</Directory>
ErrorLog \${APACHE\_LOG\_DIR}/ebrigade\_error.log
CustomLog \${APACHE\_LOG\_DIR}/ebrigade\_access.log combined
</VirtualHost>

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 163 / 197 - CHAHROUR Walid





Une fois après avoir rentré les information nécessaire nous allons activer le site ainsi que le module via les commandes suivantes :

# sudo a2ensite ebrigade.conf sudo a2enmod rewrite sudo systemctl reload apache2

billy@srv-e-brigade:~\$ sudo a2ensite ebrigade.conf sudo a2enmod rewrite sudo systemctl reload apache2 Enabling site ebrigade. To activate the new configuration, you need to run: systemctl reload apache2 Enabling module rewrite. To activate the new configuration, you need to run: systemctl restart apache2 billy@srv-e-brigade:~\$



# brigade à partir d'un navigateur

Alors une fois avoir finaliser l'installation nous allons prendre un navigateur et donc taper cette ip :

http://192.168.20.11/



# Paramétrage E-brigade

Une fois avoir taper nous allons atterrie sur cette page de configuration de base de donnée

- (1) Rentrer le nom du serveur
- (2) Rentrer l'utilisateur
- (3) Rentrer le mot de passe
- (4) Rentrer le nom de la data base
- (5) Cliquer sur valider



information

Une fois après avoir rentrer les bonne nous allons devoir changer le mot de passe



Cliquer sur Choix mot de passe pour admin









Total 13

÷

+

+

+

+

### Un autre message de confirmation





# **Fixation IP sur Ubuntu 22.04**

sudo nano /etc/netplan/00-installer-config.yaml :

BTSSIO

billy@srv-mail:~\$ sudo nano /etc/netplan/00-installer-config.yaml
[sudo] password for billy: |

- billy@srv-mail:~\$ : Invite de commande du terminal, utilisateur billy connecté sur la machine nommée srv-mail.
- sudo nano /etc/netplan/00-installer-config.yaml :
  - o Utilise sudo pour ouvrir le fichier système en tant qu'administrateur.
  - Utilise l'éditeur de texte nano pour modifier le fichier YAML de configuration réseau situé dans **/etc/netplan/**.
- [sudo] password for billy: : Le système demande maintenant le mot de passe de l'utilisateur billy pour exécuter la commande avec privilèges.

# Contenu du fichier /etc/netplan/00-installer-config.yaml



version: 2 Indique la version du format Netplan (obligatoire).

ethernets: Définit les interfaces réseau de type Ethernet.

ens33: Nom de l'interface réseau configurée (à adapter selon votre machine).

dhcp4: no Désactive l'attribution automatique via DHCP (IPv4).

addresses: Adresse IP statique assignée à l'interface.

- 192.168.20.30/24 IP statique + masque CIDR (/24 = 255.255.255.0).

routes: Définition des routes par défaut.

- to: default Route par défaut.

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 167 / 197 - CHAHROUR





via: 192.168.20.254 Passerelle (gateway) utilisée pour sortir du réseau local.

nameservers: Bloc DNS.

addresses: Liste des serveurs DNS utilisés.

- 8.8.8.8, - 1.1.1.1 DNS publics de Google et Cloudflare.

# Installation de Modoboa via Git et l'installateur

cd /opt

C'est un emplacement standard sous Linux destiné à accueillir des applications tierces ou personnalisées. Typiquement utilisé pour :

- Déployer des logiciels compilés manuellement ;
- Installer des outils comme zimbra, sonarqube, ou asterisk (hors paquets apt).

<pre>billy@srv-mail:~\$ cd</pre>	/opt
<pre>billy@srv-mail:/opt\$</pre>	

Se place dans le répertoire /opt (classiquement utilisé pour les logiciels tiers).

sudo git clone <a href="https://github.com/modoboa/modoboa-installer">https://github.com/modoboa/modoboa-installer</a>

billy@srv-mail: <b>/opt</b> \$ sudo git clone https://github.com/modoboa/modoboa-installer
Cloning into 'modoboa-installer'
remote: Enumerating objects: 3434, done.
remote: Counting objects: 100% (937/937), done.
remote: Compressing objects: 100% (259/259), done.
remote: Total 3434 (delta 784), reused 758 (delta 671), pack-reused 2497 (from 3)
Receiving objects: 100% (3434/3434), 695.79 KiB   11.79 MiB/s, done.
Resolving deltas: 100% (2386/2386), done.
billy@srv-mail:/opt\$

#### Élément Détail Permet d'exécuter la commande avec les privilèges sudo administrateur (indispensable dans /opt). git clone Clone (copie) un dépôt Git distant vers le système local. https://github.com/modoboa/modoboa-URL du dépôt Git contenant le script d'installation de la installer solution **Modoboa** (serveur de messagerie complet).

- Le dossier modoboa-installer a été créé dans le répertoire actuel (/opt). •
- Le dépôt comprend 3 434 objets, pour une taille d'environ 695 Ko, et a été transféré à 11.79 MiB/s.
- Tous les objets ont été correctement compressés, reçus et les delta (différences internes Git) ont été résolus avec succès.

Epreuve E6 – Situation professionnelle 2 - Documentation Technique - Page 168 / 197 - CHAHROUR





#### Clone le dépôt Git contenant le Modoboa Installer.

cd modoboa-installer billy@srv-mail:/opt\$ cd billy@srv-mail:/opt/mod	modoboa-installer oboa-installer\$
Élément	Explication
cd modoboa-installer	Commande utilisée pour accéder au répertoire modoboa-installer, qui vient d'être cloné depuis GitHub.
billy@srv-mail:/opt/modoboa- installer\$	Confirmation que l'utilisateur est maintenant positionné <b>dans le dossier du script d'installation</b> de Modoboa.

#### Étape suivante (logique) dans une procédure d'installation :

Il est généralement recommandé d'exécuter le script suivant :

### sudo ./run.py cod.local



### Élément

#### Description

sudo ./run.py cod.local	Lance le script principal d'installation de Modoboa avec le domaine principal cod.local.
installer.cfg not found	Le fichier de configuration n'existe pas encore, il va être généré automatiquement.
recommended to run on a FRESHLY installed server	Recommandation forte : le serveur doit être neuf, sans autres services installés pour éviter les conflits.





Élément		Description			
DNS requirements Modules installés		<ul> <li>Vous devez avoir les enregistrements suivants configurés (localement ou en DNS interne si en .local) :</li> <li>➤ mail.cod.local doit pointer vers l'IP du serveur (A record)</li> </ul>			
		<ul> <li>W doit avoir une entree MX pointant vers mail.cod.local.</li> <li>Le script va installer toute la pile mail complète, notamment :</li> <li>Sécurité : fail2ban, postwhite, opendkim</li> <li>MTA/IMAP : postfix, dovecot</li> <li>Antispam/antivirus : amavis, clamav, spamassassin, razor</li> <li>Webmail/portail : modoboa, nginx, uwsgi, automx, radicale</li> </ul>			
Do you con	ıfirm?	Vous avez validé l'installation complète en répondant y.			
Starting		Le processus d'installation est en cours. ႔ Cela peut prendre plusieurs dizaines de minutes.			
Une fois terminer voici le résultat .	Installing dovecot User dovecot already exist Congratulations! You can e Modoboa is a free software You like the project and w Then don't wait anymore an https://github.com/sponsor	s, skipping creation but please make sure the /srv/vmail directory exists. njoy Modoboa at https://mail.cod.local (admin:password) maintained by volunteers. want it to be sustainable? d go sponsor it here: rs/modoboa			

billy@srv-mail:/opt/modoboa-installer\$

# **Configuration du DNS pour modoboa**

_	🗸 😴   🚩 Gérer 🚺 Afficher Aide
	Analyseur de performances
	Centre d'administration Active Directory
	Configuration du système
	Défragmenter et optimiser les lecteurs
	Diagnostic de mémoire Windows DNS 2 Domaines et approbations Active Directory
	Éditeur du Registre
	Gestion de l'ordinateur
	Gestion des stratégies de groupe
	Informations système

Cliquez sur l'onglet **Outils** (en haut à droite de la fenêtre principale du Gestionnaire de serveur).
 (Encadré en bleu avec le repère 1) dans la capture)

2. Dans le menu déroulant, sélectionnez l'élément **DNS**.

(Encadré en rouge avec le repère (2) dans la capture)





### Structure affichée dans la console DNS :

- SRV-AD Le serveur DNS (nom de l'hôte du contrôleur de domaine).
- Zones de recherche directes Regroupe les zones DNS pour la résolution de noms → IP.
- COD.local La zone de recherche directe utilisée pour votre domaine local (cod.local).

Se Al Di Se	<ul> <li>DNS</li> <li>SRV-AD</li> <li>Cones de recherche directes</li> <li>Consides CODJocal</li> <li>Cones de recherche imversée</li> <li>Conside recherche imversée</li> <li>Pointé d'approbation</li> <li>Redirecteurs conditionnels</li> </ul>	Nom 	Type Source de nom (Si Serveur de noms ( Hôte (A) Hôte (A) Hôte (A) Hôte (A) Hôte (A) Hôte (A) Hôte (A)	Données DA) [189], srv-ad.co NS) srv-ad.cod.loca NS) srv-ad.cod.loca 192.168.10.50 192.168.10.30 192.168.10.10 192.168.10.10 192.168.10.10 192.168.10.30
			Hote (A)	192.108.10.30

Dans le panneau de droite, on observe plusieurs enregistrements de type A (adresse IPv4) déjà définis.

	Mettre à jour un fichier de données du serveur	
	Charger à nouveau	
C	Nouvel hôte (A ou AAAA) 2	
C	Nouvel hôte (A ou AAAA)       2         Nouvel alias (CNAME)       Nouveau serveur de messagerie (MX)         Nouveau domaine       Nouveau domaine         Nouveau defégation       Nouveaux enregistrements         DNSSEC       Toutes les tâches         Actualiser       Exporter la liste         Affichage       Réorganiser les icônes         Aligner les icônes       Propriétés         Aide       Nouveau	>
		Mettre à jour un fichier de données du serveur Charger à nouveau Nouvel hôte (A ou AAAA) Nouvel alias (CNAME) Nouveau serveur de messagerie (MX) Nouveau domaine Nouveau

mail.cod.local via une résolution DNS interne.

### Création d'un enregistrement de type A pour Modoboa

l'arborescence DNS (repère (1)) 2. Sélectionner **"Nouvel hôte (A ou AAAA)..."** dans le menu contextuel (repère (2))

1. Clic droit sur la zone COD.local dans

• Ajouter un **enregistrement A** pointant un **nom de machine** (ex. mail) vers une **adresse IP** (ex. 192.168.20.30).

• Indispensable pour permettre aux clients et serveurs d'**atteindre** 





Nom

\_msdcs \_sites \_tcp \_udp

Domain ForestDr

(identiq (identiqu

identiqu) (identiq

(identiq

(identiq

(identiq DESKTO

srv-ad

mail

<

SRV02-A

- (1) Nom (utilise le domaine parent si
- (2) Adresse IP (IP machine modobo) :
- (3) Valide la création de l'enregistrem

<b>n</b> (utilise le domaine narent si ce	, ch	ar	n est vide) ·	Nouvel hôte		×
		um	pest videy.	Nom (utilise le domaine parent si d	e champ est vir	
esse IP (IP machine modobo) :				mail	e champ est vic	
de la création de l'enregistreme	nt	A.				
				Nom de domaine pleinement quali	fié (FQDN) :	
				mail.COD.local.		
				Adresse IP :	a alata a ta	a dala a
				192.168.20.30 IP m	achine m	odobo
				Créer un pointeur d'enregistre	ment PTR asso	tié
				Autoriser tout utilisateur ident	ifié à mettre à i	our les
				enregistrements DNS avec le r	nême nom de pr	opriétaire
un enregistrement de type M	х	ກດເ	ır Modoboa			
— ц	2	ĸ	(1) Clie dreit			
Mettre à jour un fichier de données du senjeur		L	(1) Clic droit			
Charger à nouveau			sur la zone	3 Ajouter	un hôte	Annuler
Nouvel hôte (A ou AAAA)		_	COD.local			
Nouvel alias (CNAME)				11		
Nouveau serveur de messagerie (MX) 2						
Nouveau domaine			(2) Sélection de	e l'option : Nouveau serv	/eur de me	ssagerie
Nouvelle délégation			(MX)			
Nouveaux enregistrements			(			
DNSSEC	>	l.cc				
Toutes les tâches	>	6 <b>0</b> 0				
Actualiser		d.lc				
Exporter la liste		0				
Affichage		0				
Amenage		0				
Réorganiser les icônes	>	9				
Aligner les icônes		0				
Proprietes		0				
Aide			Nouvel enregistrement de re	essource	×	
			Serveur de messagerie (MX)			
		>	Hôte ou domaine enfant			
(1) Hôte ou domaine enfant			mail			(repère
(1)			Par défaut DNS utilise le nor	n de domaine parent lors de la création d'un e	nregistrement	
			de courrier Exchange. Vous p	pouvez spécifier un nom d'hôte ou d'enfant m	ais dans la	
(2) Nom de domaine pleineme	enτ		piupair des depioiements, le t			qualifie
(FQDN) pour le serveur de			Nom de domaine pleinement	qualifié (FQDN) :		
messagerie						
meessaberre			Nom de domaine pleinement	qualifié (FQDN) pour le serveur de messagerie		
			mail.COD.local.		Parcourir	
			Priorité du serveur de messao	gerie :		
			10			

OK

Annuler Aide

Création d'un enregistrement de type





# Accès à l'interface Web de Modoboa

Une fois que Mex est créer cliquer sur un navigateur internet puis taper le mot suivant : mail.cod.local



Barre d'adresse du navigateur (repère ①) : https://mail.cod.local Message du navigateur (Firefox ou Chrome) : Lien d'action (repère ②) : Continuer vers mail.cod.local (non sécurisé) Permet de forcer l'accès à l'interface, malgré l'avertissement de sécurité.

# Page de connexion à Modoboa (mail.cod.local)





- 1. Champ "Username" (repère 1)
  - Saisir le **nom d'utilisateur** administrateur par défaut (en général admin).
- 2. Champ "Mot de passe" (repère 2)
  - Saisir le mot de passe défini lors de l'installation.
     (Ce mot de passe est affiché dans le terminal à la fin de l'installation de Modoboa. = password )
- 3. Bouton "Se connecter" (repère ③)
  - Cliquer ici pour valider les identifiants et accéder au tableau de bord d'administration.

# Barre de navigation (haut de page) :

- Statistics, Quarantine, Domains, Identities, Modoboa, New admin
- Nom de l'utilisateur connecté : admin

# Message de bannière :

Want to check the new admin interface?

- ► Bouton : Go to Modoboa v2
- Encadré "Latest news" :
- ► Informations sur les dernières mises à jour publiées.



### Encadré "Global statistics" :

Non sécurisé   https://mail.cod.local/dashboa	rd/	A* 😥 😭
tatistics Quarantine Domains Identities M	iodoboa New admin	
	Want to check the new ad	In Interface? Go to Modoboa v2
Hello admin.		
Latest news		Features looking for sponsoring
Release: Modoboa 2.2.0	Aug. 30, 20	13
Bug fix : 2.1.2 has been released	May 3, 20	Nothing to sponsor yet.
Modoboa 2.1.0 is out!	April 26, 20	13
Modoboa @PyconFR 2023	Feb. 11, 20	13
A bunch of new releases	May 12, 20	20
Visit the officia	al weblog for more information.	
Global statistics		
Туре	Quantity	
Domains	0	
Domain aliases	0	
Identities	1	

Activer Windows accédez aux paramètres pour activer Windows.

# Accéder à la gestion des domaines dans Modoboa

L'onglet Domains (encadré rouge) est situé dans la barre de navigation supérieure, aux côtés des menus :

- Statistics
- Quarantine
- Identities
- Modoboa
- New admin





+ Add





# Ajout d'un domaine – Formulaire de création dans Modoboa

- ☑ Name (repère ①)
- ► Nom du domaine à créer : ici COD.local
- Ce domaine sera utilisé pour l'ensemble des adresses mail (ex. utilisateur@cod.local).
- ? Type
- ► Laisser sur Domain (valeur par défaut).
- ? Quota
- ► Quota global du domaine en Mo (0 = illimité).
- Default mailbox quota
- Quota par boîte mail (en Mo), attribué automatiquement à chaque utilisateur (0 = illimité).
- Image: Message sending limit
- ► Limite de mails pouvant être envoyés par utilisateur (optionnel).
- P Alias(es)
- ► Ajouter ici un ou plusieurs alias de domaine, séparés par une virgule (facultatif).
- P Enabled
- Coche activée permet l'activation immédiate du domaine.
- Inable DNS checks
- ✓ Coche activée vérifie la cohérence des enregistrements DNS (MX, SPF, etc.).
- In Enable DKIM signing
- Cochez si vous souhaitez activer la signature DKIM (recommandé en production).



New domain / Genera	1	×				
Name ?	COD.local	1				
Туре	Domain 🗸					
Quota ?	0					
Default mailbox quota ?	0					
Message sending limit ?						
Alias(es) ?						
Enabled ?	2		Cette sect	ion permet de définir les options		
Enable DNS checks ?	2		suppléme	ntaires liées au domaine fraîchement saisi		
Enable DKIM signing ?			. ,	×		
		New do	main / Opti	ons		
(COD.local).		Cr	eate a domain administrator ?	⊖ Yes ● No		
Cliquer sur <i>(encadré rc</i>	le bouton Submit ouge) pour valider	Name ?		admin @COD.local		
la création COD.local.	la création du domaine COD.local.			○ Yes		
		With a mailbox ?		Yes O No		
	/	Ci	reate aliases ?	Yes O No		
succès	ajoute avec			Close Previous Submit		
Statistics Quarantine	Domains Identities	Modoboa Net	w admin			
				Cliquer sur l'onglet Identities (encadré		
omains	Search			rouge) pour créer une ou plusieurs		
uotas	Name		Alias(es)	personnelles).		
age logs	cod.local			Ajout d'une identité (utilisateur)		
	۹ +	Add -		Onglet Identities → Bouton bleu <b>+ Add</b> (encadré en rouge).		
t		Tags				
		account	SuperAdmins	+Add -		
				Account		
Dans le me	nu <b>Identities</b> , clique	ez sur le bou	ıton bleu <b>+ /</b>	Add. account SuperA		

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 177 / 197 - CHAHROUR Walid



• Sélectionnez l'option Account (icône utilisateur noire).

# Création d'un compte utilisateur dans Modoboa

New account / General				
Role ?	Simple user 🗸			
Usemame ?	alicia@cod.local	1		
First name	Alicia			
Last name				
Random password ?				
Password		6		
Confirmation ?				
Enabled				
		Close Next		

### Rôle :

Sélectionner **Simple user** dans le menu déroulant. **Informations de l'utilisateur** :

- Username : alicia@cod.local
- First name : Alicia
- Last name : (optionnel, laissé vide ici)
- Password : entrer le mot de passe souhaité
- Confirmation : répéter le mot de passe

### Activation du compte :

La case **Enabled** est cochée par défaut . **Valider** :

Cliquer sur Next pour continuer la configuration du compte.

finalisation du compte mail "Alicia" :





## E-mail :

Le champ est prérempli avec l'adresse : alicia@cod.local

### Quota :

La case **"Use domain default value"** est cochée

 $\rightarrow$  Cela applique automatiquement la limite définie au niveau du domaine.

### Message sending limit :

Laisser vide pour ne pas appliquer de limite spécifique.

# Is send only :

Laisser décoché si l'utilisateur doit **recevoir** et **envoyer** des mails.

### Alias(es) :

Laisser vide si aucun alias n'est nécessaire.

### Sender addresses :

Laisser vide si l'adresse principale suffit pour l'envoi.

### Valider :

Cliquer sur **Submit** pour enregistrer et créer le compte.

Donc pour éviter tout répétition dans la manipulation réaliser pour les deux utilisateurs :

- Bob
- Prtg

New account / Mai	1	x
e E-mail	alicia@cod.local	
Quota ?		Use domain default value
Message sending limit ?		
Is send only ?		
Alias(es)?		
Sender addresses ?		
		Close Previous Submit



# **Installation PRTG depuis un navigateur web**

Dans cette partie là nous allons télécharger



**Cliquer sur l'icône Microsoft Edge** (cercle bleu-vert) située dans la barre en bas de l'écran pour lancer le navigateur.

Cliquez dans la **barre d'adresse** (comme sur ta capture). Tape cette URL



https://www.paessler.com/fr/prtg/download



Accepter les cookies Clique sur le bouton "ACCEPT COOKIES" pour faire disparaître le bandeau (repère 1). Lancer le téléchargement Clique ensuite sur le bouton "TÉLÉCHARGEMENT GRATUIT" (repère 2).

Ce bouton lance la version d'essai gratuite de 30 jours de **PRTG Network Monitor**.

- Saisir ton adresse e-mail professionnelle le champ indiqué (repère 1), adresse, par exemple : contact@billy-trinh.fr
- Soumettre le formulaire sur le bouton "SOUMETTRE"
   2).



### tape de confirmation : téléchargement

en cours

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 180 / 197 - CHAHROUR Walid


#### Merci d'avoir téléchargé PRTG.



Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 181 / 197 - CHAHROUR Walid



Installation - PRTG Network Monitor			- 0	>
Votre adresse email			PAESSLER	
Fournissez les informations suivantes po	our poursuivre l'installation	i -	NÉTW MONI	/OR TOF
Saisissez votre adresse e-mail. PRTG env vous alerter lorsque les capteurs de vot ou des problèmes critiques du système.	verra à cette adresse des n re installation détectent de	otifications import es pannes, des vale	antes pour urs suspecte	es,
Votre adresse email :				
prtg@cod.local 1				
Paessler vous enverra également à cette Vous pouvez à tout moment vous désin privacy@paessler.com. Nous protégeor	e adresse des informations scrire de la réception de ce 1s vos données personnelle	sur nos produits e es informations en es.	t services. écrivant à	
Consultez notre politique de confidenti	alité pour en savoir plus.			

- Le mode Rapide (recommandé) est sélectionné par défaut — garde cette option sauf si tu veux une configuration spécifique.
- 2. Clique sur **Suivant** pour continuer l'installation de PRTG.

1. Vérifie que l'adresse saisie est correcte (ici :
prtg@cod.local) – elle sera utilisée pour les
alertes.

2. Clique sur **Suivant** pour continuer l'installation.

Installation - PRTG Network Monitor	- 🗆 ×
Mode d'installation	
Choisissez entre le mode d'installation rapide ou personnalisé.	NETWORK MONITOR
Rapide (recommandé)	
<ul> <li>Utilisez le répertoire d'installation et le répertoire de données pa</li> <li>Exécutez immédiatement une découverte automatique du réseat protocoles standard (ICMP, SNMP, et autres)</li> <li>Affichez tous les équipements disponibles après le lancement de</li> <li>Modifiez la configuration du système de supervision ultérieurem</li> </ul>	ar défaut u en utilisant les e l'application ent dans l'interface Web PRT
<ul> <li>Personnalisé         <ul> <li>Choisissez manuellement le répertoire d'installation et le répertoi</li> <li>Configurez ou passez la découverte automatique du réseau</li> <li>Modifiez la configuration du système de supervision ultérieurem</li> </ul> </li> </ul>	vire de données ent dans l'interface Web PRT
www.paessler.com	Suivant Annuler

L'installation de **PRTG Network Monitor** est en cours — la barre de progression montre la **décompression des fichiers**.

N Installation - PRTG Network Monitor	-	• ×
Installation en cours Veuillez patienter pendant que l'assistant installe PRTG Network Monitor sur votre ordinateur.		PAESSLER PRTG NETWORK MONITOR
Décompression des fichiers		
www.paessler.com		

Installation en cours, tout se passe bien. Il suffit maintenant d'attendre que la décompression et l'installation se terminent.

Parfait, l'interface Web de **PRTG Network Monitor** est bien lancée sur l'adresse locale <u>http://127.0.0.1/home</u>



ONITOR



base,

PRTG Network Monitor

MONITOR

#### Le serveur PRTG est en cours d'initialisation.

Il passe différentes étapes :

Initialisation de la licence Lancement du Core Server

Chargement des définitions de modèles, types de capteurs, etc.

### **Connextion depuis l'interface WEB**

Nous sommes, arrivé à l'écran de connexion de l'interface Web de PRTG Network Monitor

127.0.0.1/hom



Bienvenue Administrateur s





#### État général :

Sonde locale (poste sur lequel PRTG est installé)  $\rightarrow$  capteurs OK mais quelques alertes jaunes (= avertissements).

DNS/ADS SRV-AD (192.168.10.30)

: Supervision active (Ping, DNS v2, HTTP...).

**Passerelle (192.168.10.254)** : Suivie avec SSL, DNS, HTTPS.

Équipements détectés :

Internet : Ping et HTTP OK. Serveurs Windows / Linux / VM : en attente d'ajout. 192.168.10.60 (Linux/Unix) : supervisé par Ping.



On peut voir que tous mes appareils sont bien remonté y compris les routeur qui sont dans les équipements inconnus



Identification des 2 routeurs en renommant

### **Configuration des mails remontant**

Dans cette partie nous allons configurer les remonter d'alerte et tester avec un compte utilisateur pour voir si ça communique bien



Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 184 / 197 - CHAHROUR Walid





Les options possibles dans cette onglets :

#### . Gérer les utilisateurs et rôles

- Ajouter ou modifier des comptes utilisateurs.
- Attribuer des rôles (Simple user, Read-only, Admin...).

#### 2. Modifier les notifications

• Définir des alertes email, SMS, ou autres (quand un capteur est en erreur, par exemple).

#### 3. Configurer les sondes

- Gérer les sondes locales ou distantes.
- Ajouter une nouvelle sonde distante si tu surveilles plusieurs sites.

#### 4. Définir des modèles de capteurs

• Pour appliquer rapidement un ensemble de capteurs prédéfinis sur plusieurs équipements.

#### 5. Paramètres système

• Modifier l'adresse IP d'écoute, le port Web, les langues, etc.

#### 1. Gérer les utilisateurs et rôles

- Ajouter ou modifier des comptes utilisateurs.
- Attribuer des rôles (Simple user, Read-only, Admin...).

#### 2. Modifier les notifications

• Définir des alertes email, SMS, ou autres (quand un capteur est en erreur, par exemple).

#### 3. Configurer les sondes

- Gérer les sondes locales ou distantes.
- Ajouter une nouvelle sonde distante si tu surveilles plusieurs sites.

#### 4. Définir des modèles de capteurs

• Pour appliquer rapidement un ensemble de capteurs prédéfinis sur plusieurs équipements.

#### 5. Paramètres système

• Modifier l'adresse IP d'écoute, le port Web, les langues, etc.







#### Configuration de l'envoi de mails via SMTP dans PRT

Système de	Transmission via SMTP	Système de transmission 🔍	O Utiliser la transmission directe avec le serveur de messagerie intégré (par défaut) O Utiliser un serveur relais SMTP (recommande pour les LAN/NAT) O Utiliser deux serveurs de relais SMTP (serveur principal et de secours)	
		Adresse email de l'expéditeur 🔍	prtg@cod.local	
		Nom de l'expéditeur 🕚	PRTG	
	0	Identification HELO	mail.cod.local	
	-	Serveur relais SMTP 🖲	192.168.20.30 Serveur modoboa	
		Port du relais SMTP 🖲	25	Enregistrer
		Authentification du relais SMTP 🖲	O Ne pas utiliser d'authentification (par défaut) Utiliser l'authentification standard SMTP Utiliser l'authentification SASL	

transmission :

Utiliser un serveur relais SMTP (recommandé pour les LAN/NAT) Détails de la configuration SMTP : Adresse email de l'expéditeur : prtg@cod.local Nom de l'expéditeur : PRTG Identification HELO : mail.cod.local Serveur relais SMTP : 192.168.20.30 (adresse IP de Modoboa) Port du relais SMTP : 25 Authentification SMTP : Utiliser l'authentification standard SMTP

### **Incident résolut**

Attention : Par défaut, le port SMTP 25 est utilisé dans la configuration de l'envoi de mails via le serveur relais (ici Modoboa : 192.168.20.30).

Cependant, **ce port est souvent bloqué ou filtré** par les fournisseurs ou les pare-feux, ce qui peut empêcher l'envoi ou la réception des messages.



## BLZZIO

Identification HELO	mail.cod.local				l est donc recommandé e port 587, qui est le po	de remplacer le port 25 po rt standard pour l'envoi de	ar
Serveur relais SMTP 🖲	192.168.20.30	Ser	veur modoboa	r - 7	mails avec authentificati	ion SMTP sécurisée	-
Port du relais SMTP 🕚	25			(•	STANTILSJ.		
Paramètres d'auther	ntification S	SMT	Р		Serveur relais SMTP 🖲	192.168.20.30	
		Aut	thentification du relais SMTP 🖲	C C	Port du relais SMTP 🖲	587	
	0		Nom d'utilisateur du relais SMTP	prtg@co	od.local		
			Mot de passe pour le relais SMTP <sup>©</sup>	Testap04	4@	λ	8
			Sécurité des connexions <sup>®</sup>	Utilis Ne p	ser SSL/TLS si pris en charge par le serveur (par défaut) pas utiliser de sécurisation de connexion	] 2	
			Méthode SSL/TLS 🔍	Nég	ociation automatique (TLS 1.0 ou version ultérieure)	] 3	
				OTLS	1.0		
				OTLS	1.2		
				OTLS	1.3		
			Tester les paramètres SMTP		Tester les para	amètres SMTP	

#### 1. Authentification du relais SMTP :

• Utiliser l'authentification standard SMTP

#### 2. Identifiants SMTP :

- Nom d'utilisateur : prtg@cod.local
- Mot de passe : Testap04@
- 3. Sécurité des connexions :
  - Utiliser SSL/TLS si pris en charge par le serveur (par défaut)

#### 4. Méthode SSL/TLS :

• Négociation automatique (TLS 1.0 ou version ultérieure)



egi

### **Test envois**

BTSSID

#### Tester les paramètres SMTP

Cela va	Méthode SSL/TLS 🖲	<ul> <li>Négociation automatique (TLS 1)</li> <li>SSLv3</li> <li>TLS 1.0</li> <li>TLS 1.1</li> <li>TLS 1.2</li> <li>TLS 1.3</li> </ul>	1.0 ou version ultérieure)	Enr
ste	er les paramètres SMTP		Tester les paramètres SMTP	

permettre à PRTG de vérifier si la connexion au **serveur Modoboa (192.168.20.30)** fonctionne correctement en utilisant :

- l'adresse d'expéditeur prtg@cod.local
- le mot de passe Testap04@
- la méthode d'authentification standard SMTP
- la négociation TLS automatique sur le port 25

#### Si tout est correct :

Tu devrais voir un message de confirmation indiquant que le test SMTP a réussi.

#### Si le test échoue :

Tu recevras une erreur du type "authentication failed" ou "unable to connect to SMTP server", auquel cas il faudra :

- vérifier l'ouverture du port 25 sur le pare-feu du serveur Modoboa
- vérifier que l'utilisateur prtg@cod.local existe bien dans Modoboa avec le bon mot de passe
- activer l'authentification SMTP sur Modoboa si ce n'est pas déjà le cas

Détail du test :

- Adresse email de destination : alice@cod.local
- Objet : Ceci est un email de test envoyé par PRTG
- L'expéditeur configuré dans les paramètres SMTP est prtg@cod.local



En cliquant sur **"OK"**, PRTG va tenter d'envoyer ce mail via le serveur Modoboa (192.168.20.30).



En cas d'échec, il faudra consulter :

- PRTG : Logs > Événements du système > Notifications
- Modoboa (Postfix) : /var/log/mail.log

## Vérification depuis l'interface WEB Modoboa

**Ouvrer Modoboa** via l'URL https://mail.cod.local : c'est bien ce qu'il faut faire pour accéder à la messagerie web et vérifier si le mail de test envoyé depuis PRTG a bien été reçu.



Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 189 / 197 - CHAHROUR Walid



## BLZZIO

Nous sommes sur le point de te connecter à l'interface Modoboa avec l'utilisateur alicia@cod.local.



Nous sommes dans les paramètres de profil de l'utilisateur Alicia dans l'interface Modoboa. Nous pouvons faire :

mettre à jour le nom affiché.

Language : tu peux passer l'interface en français si besoin.

Phone number / Secondary email : facultatif mais utile pour les notifications ou récupérations.

Quarantine Webmail Contact	s Calendars		
Auto-reply message Forward	Profile Update your personal information		
Preferences	First name	Alicia	Cliquer sur Webmail pour accéder à la boite
Security	Last name		mail
	Language ?	english	
	Phone number		
	Secondary email ?		
	Old password		
	New password		L'anacil de test <b>"Cesi est un empil de test</b>
	Confirmation		
	l	Update	envoye par PRIG" est bien arrivé dans la

Epreuve E6 – Situation professionnelle 2 -Documentation Technique - Page 190 / 197 - CHAHROUR Walid





capteur

boîte de réception de alicia@cod.local, ce qui confirme que : Le relais SMTP via Modoboa fonctionne PRTG est correctement configuré pour envoyer des notifications La boîte mail reçoit bien les alertes

Compose	C Search Q B 2 Actions -	
🕰 Inbox (1)	口 ☆ Ceci est un email de test envoyé par PRTG Mo	nday, 12:11 p.m.
Drafts	prig	% 42.8 KB
<u>●</u> Junk		

### **Configuration capteur alerte**

Pour créer une alerte personnalisée dans PRTG Network Monitor, commencez par accéder à l'équipement sur lequel vous souhaitez appliquer une alerte.



#### Aller dans le menu latéral gauche.

Cliquer sur **Équipements** (1). 1.

2. Puis sélectionner Tous (2) pour afficher l'ensemble des équipements surveillés.

Déclencheurs de notifications

Nous sommes dans l'onglet Déclencheurs de

notifications, ce qui signifie que tu vas pouvoir créer ou modifier une règle d'alerte dans PRTG.

Paramètres

Pour configurer une alerte sur un spécifique : Sélectionner un capteur (par exemple

Load, etc.).

Cliquer sur l'onglet Déclencheurs de

notifications, situé en haut à droite de la

Q Recherche Ping, CPU Find o θ the mo experi fenêtre. Cet onglet permet de définir les conditions qui déclencheront une notification : par exemple, si un

capteur passe en état d'erreur ou reste en panne pendant un certain temps.

tion

Nous sommes sur l'écran de gestion des déclencheurs de notifications pour un capteur. Voici comment comprendre et ajuster ce qui s'y trouve :



Туре 🕈	Règle	Actions
Déclencheur sur état (ID: 1)	Lorsque le statut du capteur est Erreur pendant au moins 600 secondes, exécuter @ > Notification par email et message Push à l'administrateur 🗹 Lorsque le statut du capteur est Erreur pendant au moins 900 secondes, exécuter aucune notification et répéter l'opération toutes les 0 minutes	
	Lorsque le capteur quitte le statut Erreur, exécuter 🐵 > Notification par email et message Push à l'administrateur 🖉	

Lorsque le capteur est en **Erreur pendant 600 secondes** (soit 10 minutes), il **envoie un e-mail et un push** à l'administrateur.

Si l'erreur persiste **pendant 900 secondes supplémentaires**, il **n'effectue plus d'action**. Dès que le capteur **quitte l'état d'erreur**, il **renvoie une notification** (retour à l'état normal).

Nous avons bien modifié le **déclencheur de notification** pour qu'il se déclenche **après seulement 5** secondes d'état "Erreur".

Règle	
Lorsque le statut du capteur est Erreur	pendant au moins 5 secondes, exécuter
@ > Notification par email et message Push à l'a	administrateur
Lorsque le statut du capteur est Erreur pendant au n	moins 900 secondes, exécuter aucune notification 🔻 et répéter l'opération toutes les 0
minutes	
Lorsque le capteur quitte le statut Erreur, exécuter	🖉 🕨 Natification par amail at magazara Duch à l'administratour. 🗴

Pourquoi ce réglage est utile ?

Ce type de configuration permet de :

- Être alerté quasi immédiatement en cas de panne ou d'incident critique.
- Réagir plus rapidement (ex : intervention manuelle ou redémarrage automatique via script).
- S'assurer que l'équipe d'administration reçoit bien la notification sans attendre.

### DataTel

# BTSSID

## Application de règle à un appareil spécifique pour le test

Associer le déclencheur de notification à un hôte ou un équipement afin de recevoir des alertes en cas de panne ou comportement anormal.

#### Accéder à la liste des équipements Depuis le menu principal, cliquer sur « Équipements ».

Page d'accueil	Équipements	
k éssissents		

Le capteur **Ping** surveille la disponibilité réseau de l'équipement. En cas d'inaccessibilité (perte de ping), une notification est essentielle pour intervenir rapidement.







Déclencheurs de notifications					0
	Туре 🗖	Règle		Actions	
	(aucun déclencheur défi	ni)			

Nous sommes maintenant à l'étape clé de l'ajout du déclencheur.



Depuis le capteur ciblé (ex. **Ping** de 192.168.10.251), cliquez sur :

#### • Ajouter un déclencheur sur état

Cela permet de générer une alerte dès que le capteur rencontre un changement d'état (par exemple : Erreur, Avertissement, Inhabituel).

Ce type de déclencheur est idéal pour la supervision **en temps réel** de la disponibilité réseau.

Nous sommes en train d'appliquer la règle de notification à votre capteur sélectionné. Voici comment résumer cette étape dans un ton professionnel pour votre documentation :

Accéder à l'onglet **Déclencheurs de notifications** depuis le capteur ciblé.

Cliquer sur Ajouter un déclencheur sur état.



#### Création d'un modèle de notification – Alerte Ping

Pour une meilleure gestion des alertes, nous créons un modèle dédié aux incidents détectés par le capteur Ping.

Paramétrages de base Nom du modèle Alerte ping Balises		
Statut de supervision  Actif (par défaut) En pause		
Planning © Aucun		~
Recueillir les notifications et les envoyer une fois le modèle réactivé (par défaut)     Rejeter les notifications pendant le statut de pause		
Résumé des notifications Méthode  Toujours aviser immédiatement, ne jamais résumer		2
	Annuler	Créer

Nom du modèle : Entrer un nom explicite, par exemple Alerte ping (voir image point 1). Laisser le **Statut de supervision** sur Actif (par défaut), sauf si le modèle ne doit pas être actif immédiatement.

Dans la section **Gestion des notifications lors** d'une pause planifiée, conserver l'option : Recueillir les notifications et les envoyer une fois le modèle réactivé pour ne rien perdre des événements.

#### Activation de l'envoi de notifications par email

Pour que le modèle *Alerte ping* envoie un message en cas de déclenchement, il faut **activer explicitement** l'option d'envoi par email





#### Étapes :

1. Activer l'option "Envoyer un email" en cliquant sur le bouton à bascule (voir l'encadré rouge sur l'image ci-dessus).



Ce modèle a pour but d'envoyer une notification par email lorsqu'un capteur de type **Ping** entre dans l'état "Erreur" ou retrouve un état "OK". Il permet d'être alerté rapidement en cas d'indisponibilité réseau.

Ajouter un modèle de notification	on	×		
$\bigcirc$				
Envoyer à l'utilisateur, Envoyer au gru utilisateur, groupe d'utilisateurs ou ad	oupe d'utilisateurs et Envoyer à l'adresse email fonctionnent simultanément. Chaque resse email que vous définissez ici recevra la notification.			
Envoyer à l'utilisateur 🕚				
Aucun		$\sim$		
Envoyer au groupe d'utilisateurs 🖲				
Aucun		~		
Envoyer à l'adresse email 🕚	0			
prtg@cod.local	•			
Objet 🖲				
[%sitename] %device %name %status	: %down (%message)			
Format 🖲				
Texte				
O Texte personnalisé				
Priorité				
Très élevé	0	~		
	<u>Annuler</u> Crée			
aramètre	Valeur			
om du modèle	Alarta ning			
Alerte pillg				
1				

Alerte ping				
Email				
Adresse de destination prtg@cod.local				
[%sitename] %device %name %status %down (%message)				
HTML				
Très élevé				
Aucun utilisateur / Aucun groupe				

Epreuve E6 – Situation professionnelle 2 - Documentation Technique - Page 195 / 197 - CHAHROUR



Une fois le **modèle de notification "Alerte ping"** créé, nous l'avons appliqué à un **capteur de type Ping** sur l'équipement 192.168.10.251.

Déclencheur configuré :

- Type : Déclencheur sur état
- Condition : Lorsque le capteur est en Erreur pendant 60 secondes
- Action : Exécuter la notification Alerte ping
- Répétition : Pas de répétition automatique
- Fin d'erreur : Aucune notification à la sortie de l'état Erreur

Cette configuration garantit une réactivité rapide en cas d'interruption réseau détectée par le capteur.



Une fois que l'utilisateur à cliquer sur le bouton bleu cela va enregistrer la règle

Déclencheurs de notifications	Туре 🔦	Règle	Actions
	Déclencheur sur état (ID: 1)	Lorsque le statut du capteur est Erreur pendant au moins 60 secondes, exécuter 👜 Alerte ping 🗹 Lorsque le statut du capteur est Erreur pendant au moins 300 secondes, exécuter aucune notification et répéter l'opération toutes les 0 minutes Lorsque le capteur quitte le statut Erreur, exécuter aucune notification	<ul><li>▲</li></ul>
Déclencheurs de notifications pouvant être hérités des objets parents	Hériter de tous les     Utiliser uniqueme	s déclencheurs de notifications des objets parents et utiliser les déclencheurs de notifications définis ci-dessus (par défaut) nt les déclencheurs de notifications définis ci-dessus	
Déclencheurs de notifications pouvant être hérités des objets parents	Hériter de tous les     Utiliser uniqueme     Type ^	s déclencheurs de notifications des objets parents et utiliser les déclencheurs de notifications définis ci-dessus (par défaut) nt les déclencheurs de notifications définis ci-dessus Règle	hérité de



### Conclusion – Test de déclenchement d'alerte

Ce scénario constitue un **test volontaire** visant à vérifier que le système de surveillance PRTG est capable de détecter une **perte de connectivité** et de **déclencher automatiquement une alerte** via les mécanismes configurés.

G	RTE01 × 🕅 RTE02 ×	101-AD × 🕞 SRV02-AD × [	SRV-MAIL 🗙 🕞 SRV-VOIP	X SRV-E-brigade X	🕞 CLI-WAN 🗙 🕞 CLI-	lan 🗙		
R	Racine Groupe PRTG Network X	🖂 Webmail	× +					
	COUPÉS0.1/group.htm?id=08							
					-	Nouvelles alarmes 1	Nouvelles entrées de log	g 24 <b>!! 1 W 2</b>
uei	il Équipements		iteurs	Alarmes	Cartes 3	Rapports	Logs	Tickets
T	😑 📼 Serveurs notes vinware							CONTINUE PR
	Serveurs VMware vCente							
		Webmail						
	🗆 🛱 Hyper-V	mail.cod.local						Statut:
	Hôtes Hyper-V     Ajouter u	Cet onglet a été ignoré pour ressources.	enregistrer les					ID:
	🗄 🔄 Hyper-V machines virtuel	Ajouter un équipement						
Ð	🛱 Linux / macOS / Unix							+
□ m 192.168.10.60 ↔ Ajouter un							and the second	
	0 ms	capteur						The second
	Ajouter un équipeme	ent						John
	Équipements inconnus							
	B Routours Pfsense192.168.1	0 🙆						100,0 2 10
	E = 192.168.10.251 = in p	ause par dépendance Caoteur de cer III SSL vérificatio III	DNS v2 II HTTPS	+ Ajouter un				60,0
				capteur				40,0 20.0 -
	🗆 💷 192.168.10.252 Recomm	nandation de capteurs en cours (18%)	q					0,0

- Simuler une coupure réseau en désactivant volontairement les routeurs RTE01 et RTE02.
- Observer la réaction de PRTG en termes de détection, pause des capteurs dépendants et génération d'alertes.
- Vérifier la réception des notifications (email) pour confirmer l'efficacité du modèle de notification configuré précédemment.

#### Résultats obtenus :

- Les équipements liés aux routeurs ont bien été mis en pause automatiquement.
- Le capteur de type **Ping** a basculé en état "en pause par dépendance", ce qui montre que les règles de hiérarchie et de dépendance sont bien fonctionnelles.
- Des logs et une alarme ont bien été générés.
- Le test démontre que la configuration actuelle est **opérationnelle et réactive** face à un incident de type "perte de connexion".

Ce test valide le bon fonctionnement de l'infrastructure de supervision ainsi que des notifications critiques.

#### Comportement observé après réactivation des routeurs





Après la remise en ligne des routeurs **RTE01** et **RTE02**, les capteurs associés dans PRTG sont passés brièvement en **état clignotant** (alternance entre actif et pause). Ce comportement est **normal et attendu** dans le cadre d'un test avec **délai de déclenchement configuré**.

#### Analyse :

	Ajouter un équipement	
[	E Inux / macOS / Unix E ■ 192.168.10.60 Ping 0 ms + Ajouter un capteur	<ul> <li>L'état</li> <li>"clignotant"</li> </ul>
[	<ul> <li>☐ Imprimantes</li> <li>Ajouter un équipement</li> <li>☐ Équipements inconnus</li> </ul>	reflète une <b>période</b> d'instabilité
	□ 🛱 Routeurs Pfsense192.168.10	momentanée
	□ IP2.168.10.251 □ En pause par dépendance Ping Sms □ Capteur de cer □ SSL vérificatio □ DNS v2 □ HTTPS	où le système
	🖻 💷 192.168.10.252 Recommandation de capteurs en cours (18%) 🏳	systeme
	W Ping       W Capteur de cer 397 ≢       ✓ SSL vérificatio Only Strong Prot       ✓ DNS v2 Yes       ✓ HTTPS 7116 ms <ul> <li>Ajouter un capteur</li> </ul>	confirmer le
		Telour a la
		normale.

- Cette phase de transition est influencée par les valeurs de délais définies dans les déclencheurs (ex. : 60 secondes avant exécution de la notification, ou 300 secondes pour l'arrêt).
- Dans ce cas précis, la **latence de confirmation** combinée à l'état antérieur en erreur a pu ralentir la réactivation complète des capteurs dépendants.

#### Action corrective :

Face à cette instabilité temporaire, un **redémarrage manuel des routeurs** a été effectué. Ce redémarrage a permis de **stabiliser la connectivité réseau**, entraînant le **retour à l'état "OK"** pour tous les capteurs associés.