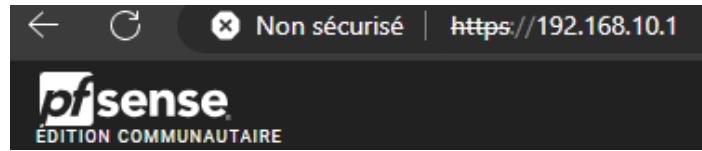


## Compte rendu mission 3

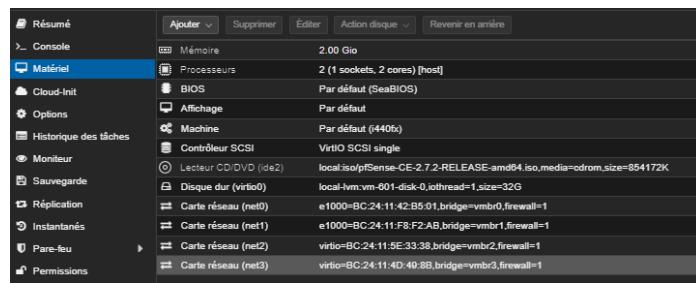
On configure les interfaces sur notre pfSense

On accéder à l'interface web de pfSense :

On se connecte à l'interface web via l'adresse IP de notre pfSense :

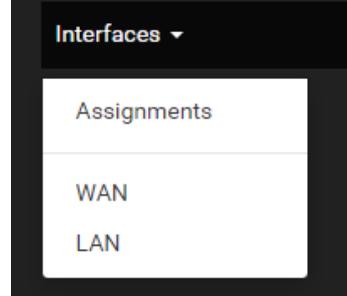


Il nous faut 4 cartes réseau  
une pour le WAN, VLAN, VLAN2 et pour la DMZ

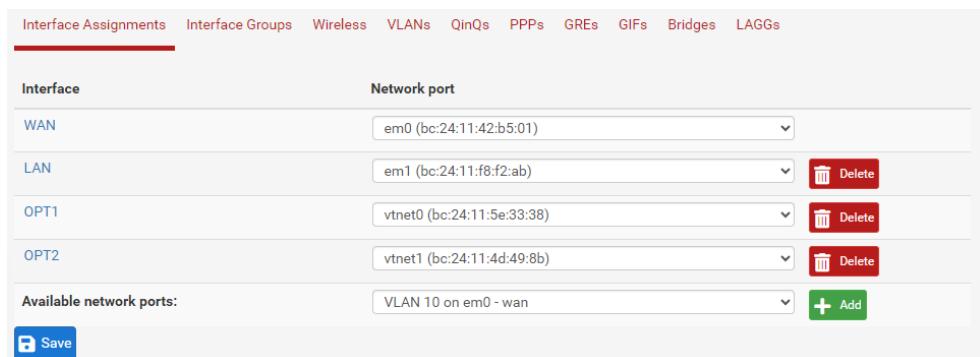


Type	Description
Mémoire	2.00 Go
Processeurs	2 (1 sockets, 2 cores) [host]
BIOS	Par défaut (SeabIOS)
Affichage	Par défaut
Machine	Par défaut (440fx)
Contrôleur SCSI	VirtIO SCSI single
Lecteur CD/DVD (ide2)	local:softfSense-CE-2.7.2-RELEASE-amd64.iso.media=cdrom.size=854172K
Disque dur (virtio0)	local-lvm.vm=801-disk-0,othread=1,size=32G
Carte réseau (net0)	e1000=BC:24:11:42:B5:01,bridge=vmbr0,firewall=1
Carte réseau (net1)	e1000=BC:24:11:F8:F2:AB,bridge=vmbr1,firewall=1
Carte réseau (net2)	virtio=BC:24:11:5E:33:38,bridge=vmbr2,firewall=1
Carte réseau (net3)	virtio=BC:24:11:4D:40:8B,bridge=vmbr3,firewall=1

On vas dans « interfaces » puis « assignments » :



Dans le menu déroulant, on voit les VLANs créer sur proxmox  
Puis on clique sur « add » pour les ajouter comme interfaces :



Interface	Network port	Action
WAN	em0 (bc:24:11:42:b5:01)	
LAN	em1 (bc:24:11:f8:f2:ab)	<span>Delete</span>
OPT1	vtnet0 (bc:24:11:5e:33:38)	<span>Delete</span>
OPT2	vtnet1 (bc:24:11:4d:49:8b)	<span>Delete</span>
Available network ports:	VLAN 10 on em0 - wan	<span>Add</span>

On configure l'adresse IP pour le LAN :  
Puis cliquer sur « save » et « apply change »

On

Interfaces / LAN (em1)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx This field can be used to modify ('spoof') the MAC address of this interface. Enter a MAC address in the following format: xxx:xxxx:xxxx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.168.10.1	/ 24
IPv4 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.

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/>	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	<input type="checkbox"/>	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. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

configure l'adresse IP pour le WAN:

On Configure le WAN pour obtenir une adresse via DHCP

Puis cliquer sur « save » et « apply change »

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	DHCP6
MAC Address	xxxxxxxxxxxx This field can be used to modify ('spoof') the MAC address of this interface. Enter a MAC address in the following format: xxx:xxxx:xxxx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

configurer l'Interface DMZ :

On coche la premiere case On renomme notre machine et on modifie l'adresse IP :

Puis cliquer sur « save » et « apply change »

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxx:xxxx:xxxx This field can be used to modify ('spoof') the MAC address of this interface. Enter a MAC address in the following format: xxxx:xxxx:xxxx or leave blank.
MTU	
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.	
MSS	
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IP header size) and minus 60 for IPv6 (TCP/IP header size) will be in effect.	
Speed and Duplex	Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.	
Static IPv4 Configuration	
IPv4 Address	192.168.30.1 / 24
IPv4 Upstream gateway	None <a href="#">+ Add a new gateway</a>
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 <a href="#">clicking here</a> .	
Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> 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	<input type="checkbox"/> 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. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
<a href="#"> Save</a>	

On configure ensuite l'interface VLAN :

**General Configuration**

Enable	<input checked="" type="checkbox"/> Enable interface
Description	VLAN20 Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxxxx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

IPv4 Address	192.168.20.1	/ 24
IPv4 Upstream gateway	None	<a href="#">+ Add a new gateway</a>
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.		

**Reserved Networks**

Block private networks and loopback addresses	<input type="checkbox"/>	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	<input type="checkbox"/>	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. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

## Configurer le Pare-feu

Accéder aux Règles de Pare-feu :

Sélectionne l'interface LAN pour créer des règles d'accès :

Cliquer sur « add » :

Firewall / Rules / LAN

Floating	WAN	<b>LAN</b>	DMZ	VLAN20							
<b>Rules (Drag to Change Order)</b>											
Actions	Description	Schedule	Queue	Gateway	Port	Destination	Source	Protocol	States		
<a href="#">Edit</a>	Anti-Lockout Rule	*	*	*	443 80	LAN Address	*	*	*	0/1.90 MiB	<input checked="" type="checkbox"/>
<a href="#">Edit</a>	Default allow LAN to any rule	none	*	*	*	LAN subnets	*	*	*	5/47.79 MiB	<input checked="" type="checkbox"/>

[Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

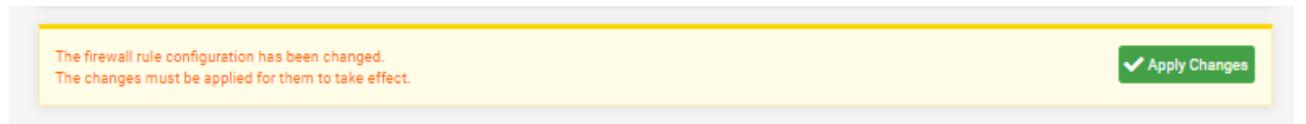
Clique sur Add et configure une règle pour permettre tout le trafic sortant du LAN vers le WAN

Clique sur Save en bas de la page.

**Edit Firewall Rule**

Action	Pass				
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.					
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.				
Interface	LAN				
Choose the interface from which packets must come to match this rule.					
Address Family	IPv4				
Select the Internet Protocol version this rule applies to.					
Protocol	Any				
Choose which IP protocol this rule should match.					
<b>Source</b>					
Source	<input type="checkbox"/> Invert match	LAN subnets	Source Address	/	▼
<b>Destination</b>					
Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	▼
<b>Extra Options</b>					
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).				
Description	Allow all LAN to WAN traffic				
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.					
Advanced Options	<input type="button" value="Display Advanced"/>				
<input type="button" value="Save"/>					

Clique sur Apply Changes (Appliquer les Changements) en haut de la page :



On ajoute une règle à la DMZ la même que celle du LAN :

Floating	WAN	LAN	DMZ	VLAN20						
<b>Rules (Drag to Change Order)</b>										
<input type="checkbox"/> States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.										
<input type="button" value="↑ Add"/> <input type="button" value="↓ Add"/> <input type="button" value="Delete"/> <input type="button" value="Toggle"/> <input type="button" value="Copy"/> <input type="button" value="Save"/> <input type="button" value="+ Separator"/>										

Cliquer sur « save » pour enregistrer puis sur apply change :

On

**Edit Firewall Rule**

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	DMZ
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any
Choose which IP protocol this rule should match.	
<b>Source</b>	
Source	<input type="checkbox"/> Invert match      DMZ subnets      Source Address /
<b>Destination</b>	
Destination	<input type="checkbox"/> Invert match      Any      Destination Address /
<b>Extra Options</b>	
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Allow all DMZ to WAN traffic A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button" value="Display Advanced"/>
<input type="button" value="Save"/>	

ajoute une règle pour l'accès à internet :  
Clique sur Save (Enregistrer) pour sauvegarder cette règle

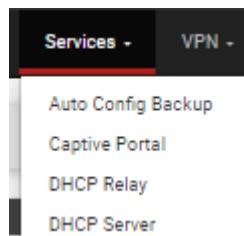
**Edit Firewall Rule**

Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.				
Disabled	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.				
Interface	DMZ	Choose the interface from which packets must come to match this rule.				
Address Family	IPv4	Select the Internet Protocol version this rule applies to.				
Protocol	TCP	Choose which IP protocol this rule should match.				
<b>Source</b>						
Source	<input type="checkbox"/> Invert match	Any	Source Address	/	<input type="button" value="Display Advanced"/>	
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.						
<b>Destination</b>						
Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	<input type="button" value="Display Advanced"/>	
Destination Port Range	From	Custom	To	Custom	Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.	
<b>Extra Options</b>						
Log	<input type="checkbox"/> Log packets that are handled by this rule	Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).				
Description	Allow DMZ web traffic					A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button" value="Display Advanced"/>					<input type="button" value="Save"/>

Une fois  
as ajouté  
les règles

nécessaires, cliquez sur Apply Changes (Appliquer les Changements) en haut de la page.

Il faut configurer le DHCP sur VLAN WIFI



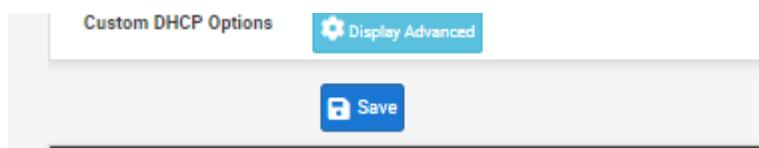
activer le serveur DHCP

Définir une étendue d'adresse allouée par le service

que tu  
toutes

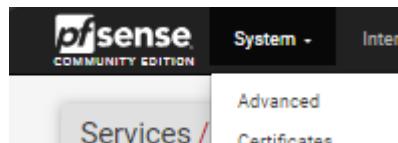
The screenshot shows the pfSense DHCP configuration for the VLAN20 interface. Under 'General DHCP Options', the 'DHCP Backend' is set to 'ISC DHCP'. The 'Enable' checkbox is checked, and 'Allow all clients' is selected under 'Deny Unknown Clients'. Under 'Primary Address Pool', the subnet is 192.168.20.0/24, and the range is 192.168.20.1 - 192.168.20.254. An additional pool section is present with a '+ Add Address Pool' button.

On enregistre les modifications :



**ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.**

Allez sur « system » puis « advanced » :



Cliquer sur « networking »

On coche la première option :

The screenshot shows the 'Networking' tab selected in the pfSense navigation. In the 'DHCP Options' section, the 'Server Backend' is set to 'Kea DHCP' (radio button selected). A note at the bottom states: 'ISC DHCP has reached end-of-life and will be removed from a future version of pfSense. Kea DHCP is the newer, modern DHCP distribution from ISC that includes the most-requested features.' There is also an 'Ignore Deprecation Warning' checkbox.

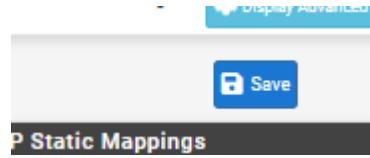
puis on coche également « enable DHCP server sur l'interface LAN »

General DHCP Options

DHCP Backend Kea DHCP

Enable  Enable DHCP server on LAN interface

Une fois terminé, cliquez sur «Enregistrer» pour enregistrer les modifications.



The DHCP Server configuration has changed.  
The changes must be applied for them to take effect.

✓ Apply Changes

créer des règles de pare-feu Pfsense :

appuyez sur le bouton Pare-feu situé dans le menu supérieur puis appuyez sur Règles

appuyez sur le bouton Ajouter comme indiqué ci-dessous.

Firewall / Rules / VLAN20

Floating WAN LAN DMZ **VLAN20**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.											

↑ Add ↓ Add Delete Toggle Copy Save + Separator

On ajoute notre règle :

**Edit Firewall Rule**

Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	VLAN20	Choose the Interface from which packets must come to match this rule.
Address Family	IPv4	Select the Internet Protocol version this rule applies to.
Protocol	Any	Choose which IP protocol this rule should match.
<b>Source</b>		
Source	<input type="checkbox"/> Invert match	VLAN20 address
<b>Destination</b>		
Destination	<input type="checkbox"/> Invert match	Any

après avoir créé une règle, appuyez sur le bouton Enregistrer pour l'enregistrer

**Extra Options**

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Autoriser Internet pour VLAN20
Advanced Options	<a href="#">Display Advanced</a>
<b>Save</b>	

Cliquez sur « Save » en bas de page pour sauvegarder et cliquez sur « Apply Changes » pour appliquer la nouvelle configuration.

The firewall rule configuration has been changed.  
The changes must be applied for them to take effect.

**Apply Changes**

Floating	WAN	LAN	DMZ	VLAN20					
<b>Rules (Drag to Change Order)</b>									
Actions	Description	Queue	Gateway	Port	Destination	Port	Protocol	Source	States
<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Toggle</a> <a href="#">Copy</a> <a href="#">Save</a> <a href="#">Separator</a>	Autoriser Internet pour VLAN20	none	*	*	*	*	IPv4 +	VLAN20 address	0/0 E

On ajoute une nouvelles règle pour ce faire on suit les captures précédentes  
On bloque l'accès du LAN vers le VLAN

**Edit Firewall Rule**

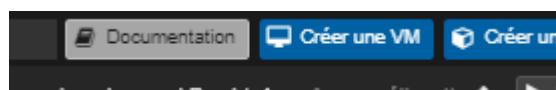
Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet ("TCP-RST" or ICMP port unreachable for UDP) is returned to the sender; whereas with block, the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	VLAN02 Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	Any Choose which IP protocol this rule should match.
<b>Source</b>	
Source	<input type="checkbox"/> Invert match    VLAN02 address    Source Address
<b>Destination</b>	
Destination	<input type="checkbox"/> Invert match    Any    Destination Address
<b>Extra Options</b>	
Log	<input type="checkbox"/> Log packets that are handled by this rule. Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status system Logs Settings page).
Description	Block access to LUN from VLAN02 A description may be entered here for administrative reference. A maximum of 255 characters will be used in the rule and displayed in the firewall log.
Advanced Options	
<a href="#">Display Advanced</a>	
<b>Save</b>	

Cliquez sur «Enregistrer» pour enregistrer les modifications.

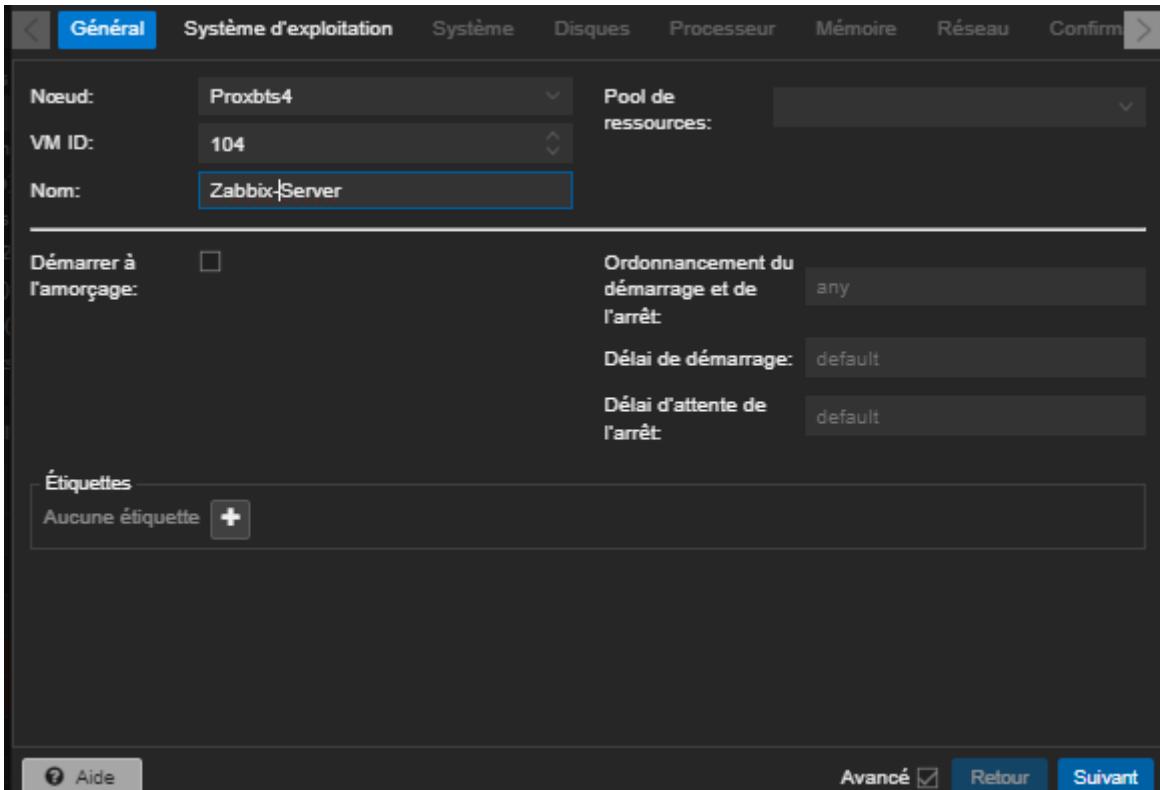


## Installer le serveur Zabbix

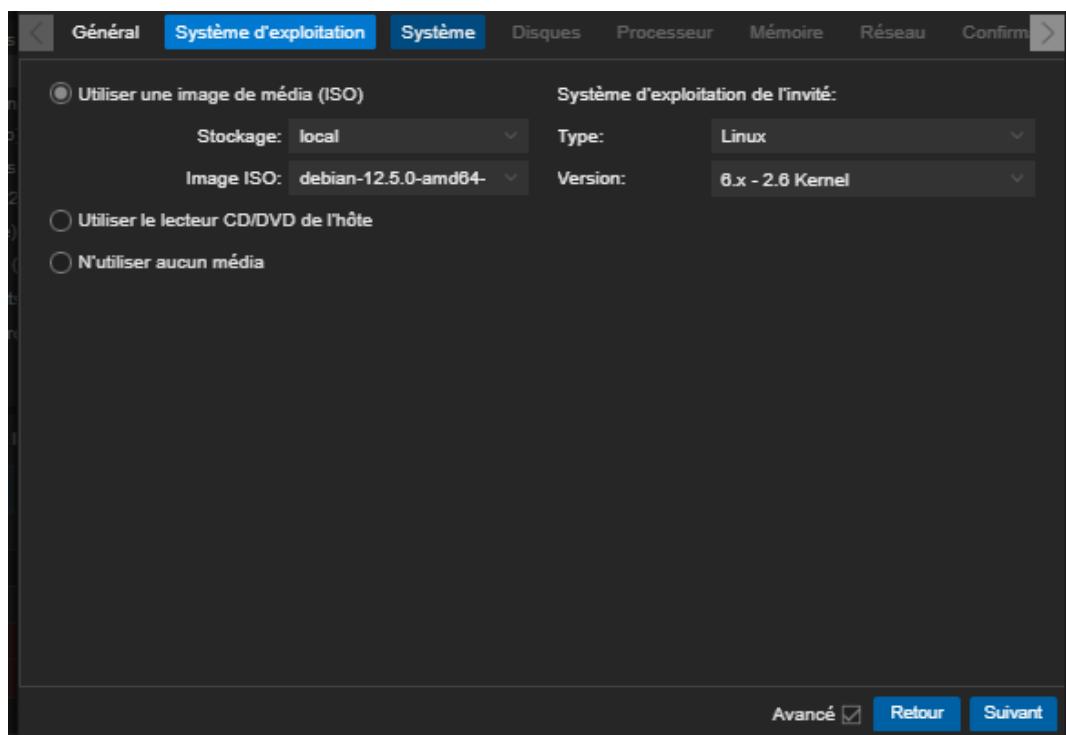
Cliquez sur le bouton Crée une VM situé dans le coin supérieur droit.



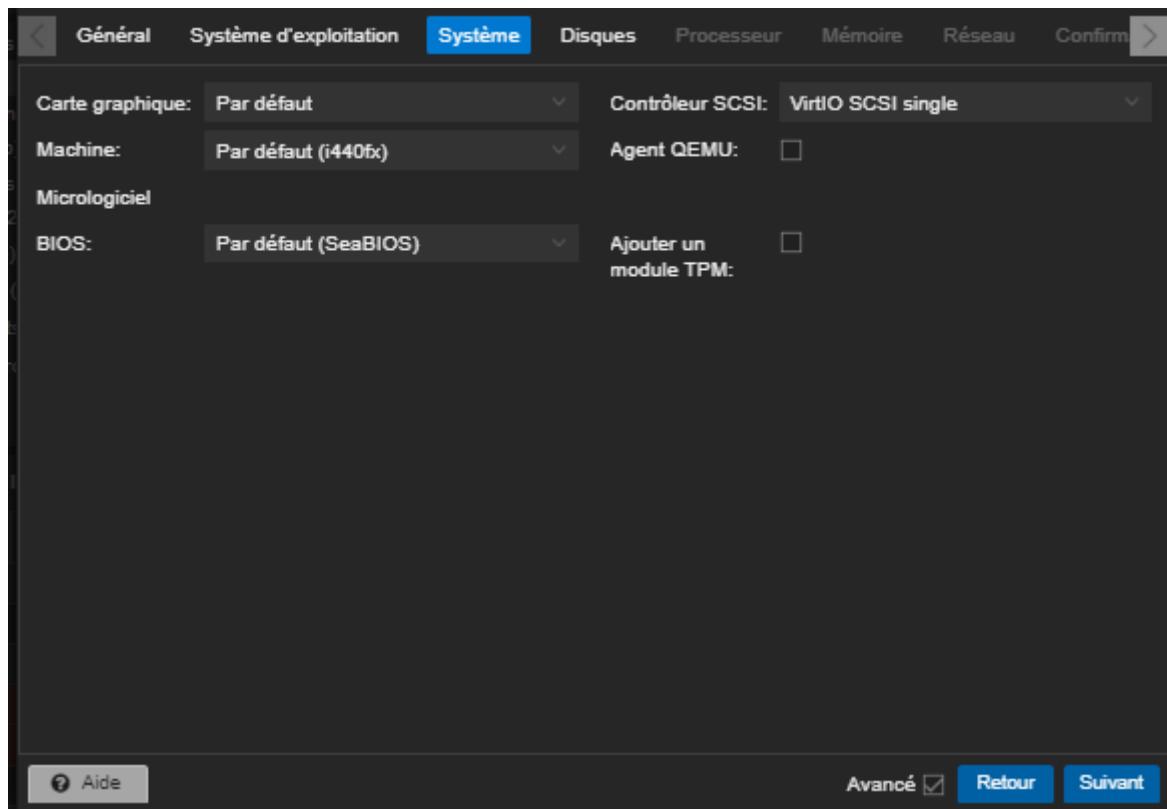
On donne un nom à notre machine virtuel en l'occurrence « Zabbix-Server »



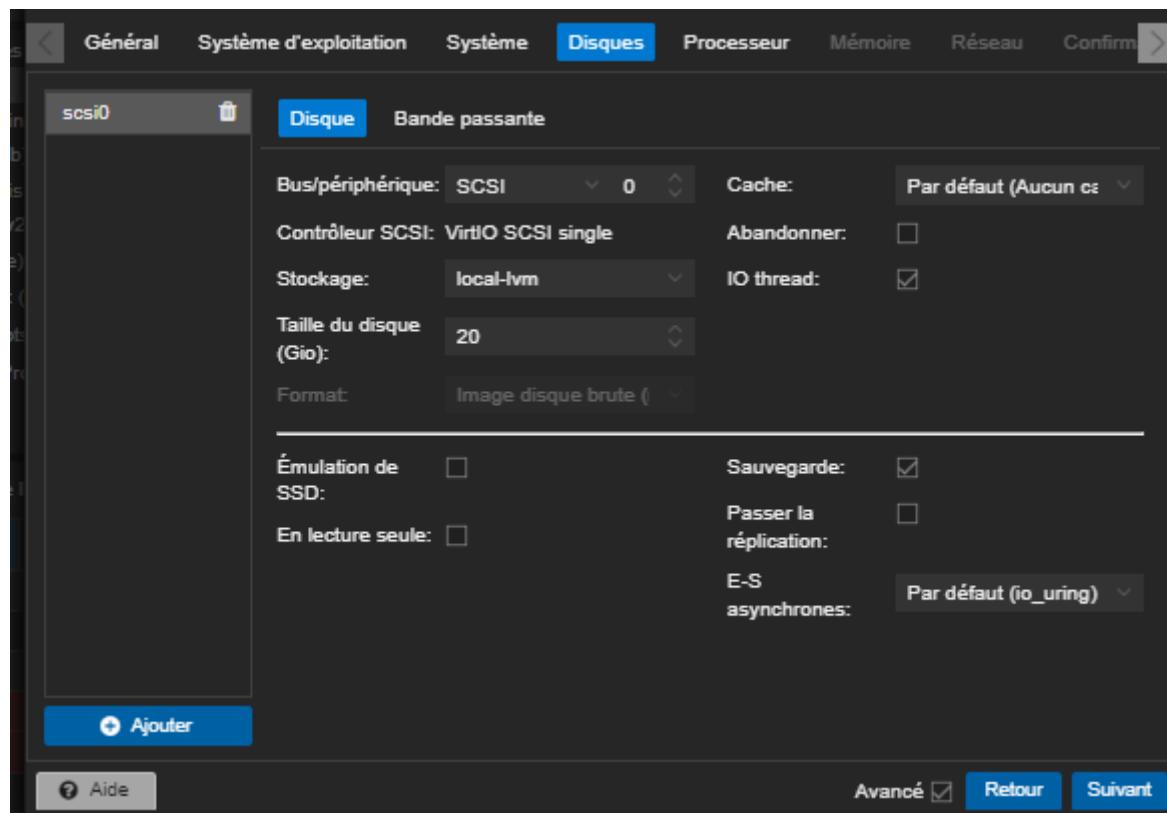
Dans la section OS, sélectionnez l'image ISO dans le menu déroulant.



cliquez sur le bouton Suivant pour continuer.



On modifie SCSI et on met SATA a la place  
On a attribué 20 Go d'espace à la machine virtuelle.



Attribuez les coeurs de processeur

Général Système d'exploitation Système Disques Processeur Mémoire Réseau Confirm >

Supports de processeur: 1 Type: host  
Cœurs: 2 Total de cœurs: 2

---

Processeurs virtuels: 2 Unités processeur: 100  
Limite d'utilisation processeur: illimité Activer NUMA:

Affinité processeur: Tous les cœurs

Extra CPU Flags:

Default	- ○○○ +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	- ○○○ +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	- ○○○ +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	- ○○○ +	ssbd	Protection for "Speculative Store Bypass" for Intel models

Aide Avancé  Retour Suivant

On attribue à cette VM 2048MB de mémoires :

Général Système d'exploitation Système Disques Processeur Mémoire Réseau Confirm >

Mémoire (MiB): 2048

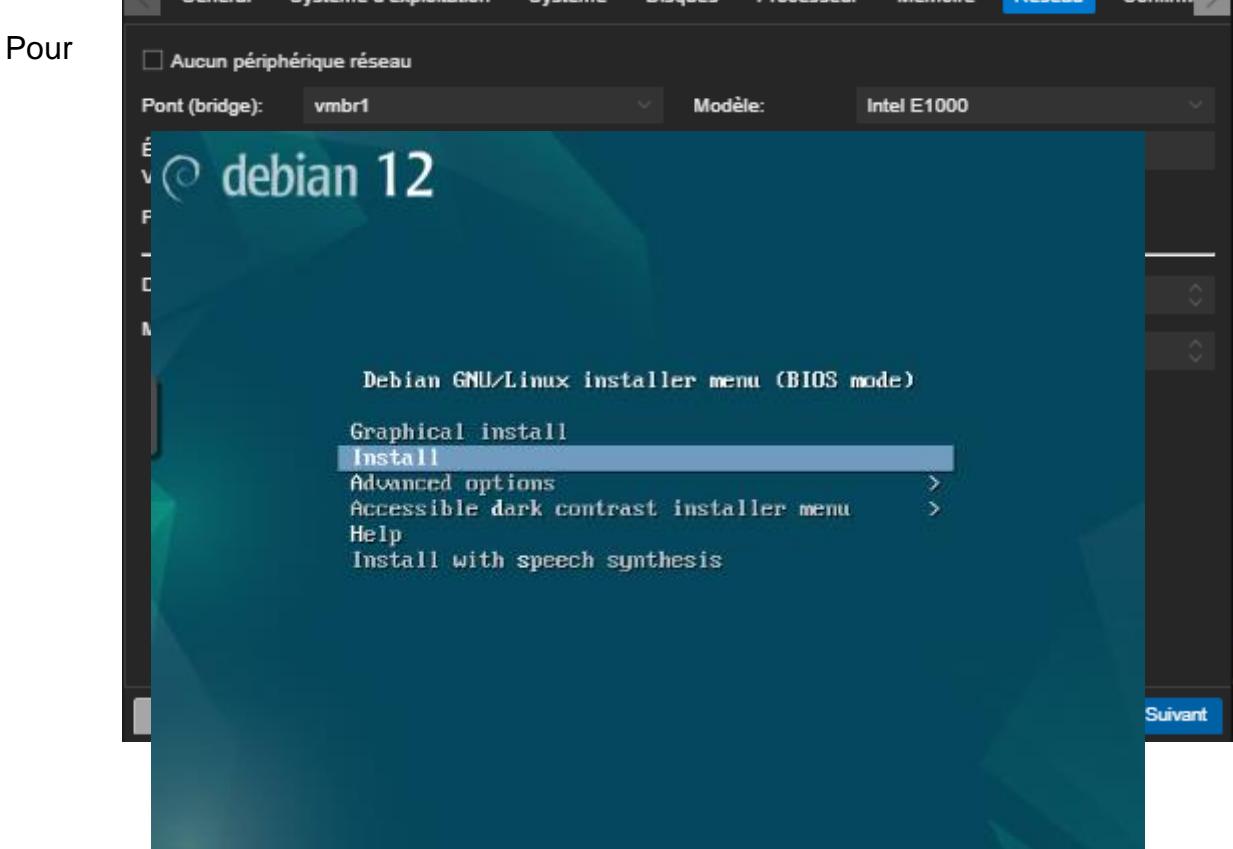
---

Mémoire minimale (MiB): 2048  
Partages: Par défaut (1000)

Élasticité mémoire (ballooning):

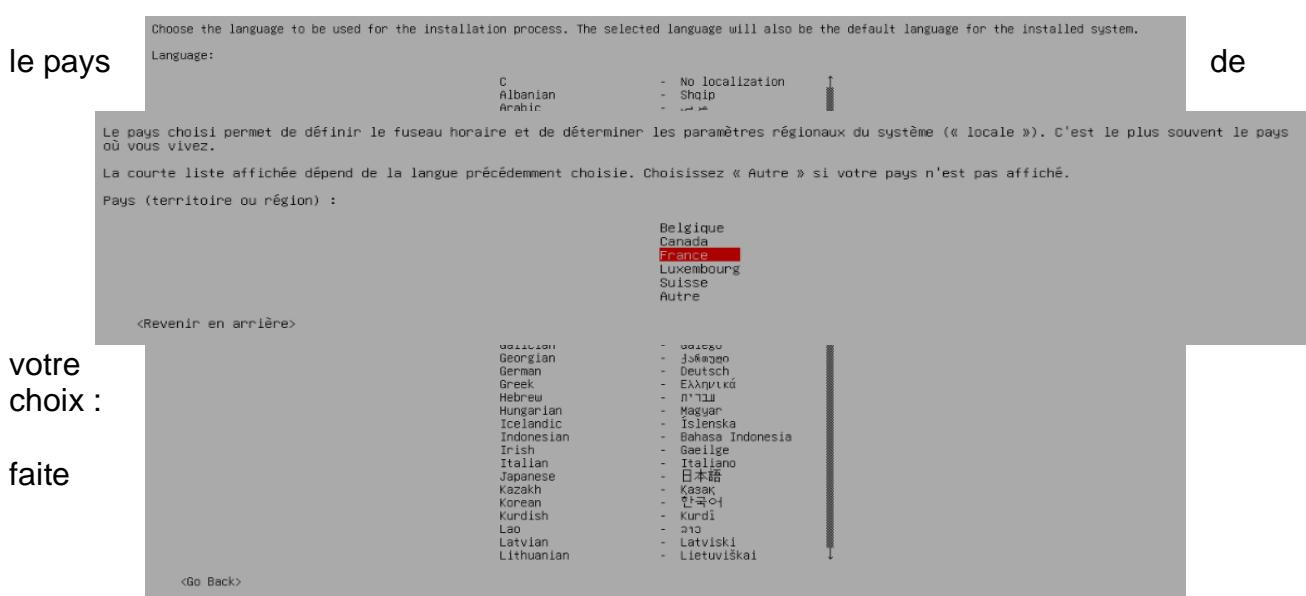
Aide Avancé  Retour Suivant

mettre en intel E100 puis confirmer l'installation de la VM



l'installation on choisie la deuxième option

choisissez la langue de votre choix :



votre  
choix :

faite

« continuer » :

Donner un nom à votre



machine :

Veuillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

debian

<Revenir en arrière>

<Continuer>

mettre un mot de passe :

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur mal intentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

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 vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les priviléges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

Mot de passe du superutilisateur (« root ») :

123

[] Afficher le mot de passe en clair

<Revenir en arrière>

<Continuer>

mettre un mot de passe pour le superutilisateur :

Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

Confirmation du mot de passe :

123

Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

donner un nom à l'utilisateur :

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veuillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

zabbix

<Revenir en arrière> <Continuer>

Fait « continuer » :

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 :

zabbix

<Revenir en arrière> <Continuer>

Mettre son mot de passe :

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

123

Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

On passe à la méthode de partitionnement

On utilise le disque entier :

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

<Revenir en arrière>

On choisie le disque a partitionner :

Veuillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.

Disque à partitionner :

SCSI3 (0,0,0) (sda) - 21.5 GB ATA QEMU HARDDISK

<Revenir en arrière>

faite « continuer » :

Disque partitionné :

SCSI3 (0,0,0) (sda) - ATA QEMU HARDDISK: 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

<Revenir en arrière>

On termine le partitionnement de la machine :

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.

Partitionnement assisté  
Configurer le RAID avec gestion logicielle  
Configurer le gestionnaire de volumes logiques (LVM)  
Configurer les volumes chiffrés  
Configurer les volumes iSCSI

SCSI3 (0,0,0) (sda) - 21.5 GB ATA QEMU HARDDISK  
n° 1 primaire 20.4 GB f ext4 /  
n° 5 logique 1.0 GB f swap swap

Annuler les modifications des partitions  
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>

On ne veut pas analyser d'autres support :

L'analyse des supports d'installation a trouvé l'étiquette :

On

Debian GNU/Linux 12.5.0 \_Bookworm\_ - Official amd64 NETINST with firmware 20240210-11:27

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 ?

<Revenir en arrière>

<Oui> <Non>

applique les changement sur le disque :

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :

SCSI3 (0,0,0) (sda)

Les partitions suivantes seront formatées :

partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4

partition n° 5 sur SCSI3 (0,0,0) (sda) de type swap

Faut-il appliquer les changements sur les disques ?

**<Oui>** **<Non>**

faite « continuer » :

faite

L'objectif est de trouver un miroir de l'archive Debian qui soit proche de vous du point de vue du réseau. Gardez à l'esprit que le fait de choisir un pays proche, voire même votre pays, n'est peut-être pas le meilleur choix.

Pays du miroir de l'archive Debian :

Saisie manuelle  
Afrique du Sud  
Allemagne  
Argentine  
Arménie  
Australie  
Autriche  
Belgique  
Brésil  
Bulgarie  
Bélarus  
Cambodge  
Canada  
Chili  
Chine  
Corée du Sud  
Costa Rica  
Croatie  
Danemark  
Espagne  
Estonie  
Finlande  
**France**  
Grèce  
Géorgie  
Hong Kong  
Hongrie  
Inde  
Indonésie  
Iran  
Islande  
Israël  
Italie  
Japon  
Kazakhstan  
Kenya

[<Revenir en arrière>](#)

continuer :

Veuillez choisir un miroir de l'archive Debian. Vous devriez utiliser un miroir situé dans votre pays ou votre région si vous ne savez pas quel miroir possède la meilleure connexion Internet avec vous.

Généralement, deb.debian.org est un choix pertinent.

Miroir de l'archive Debian :

**deb.debian.org**  
ftp.fr.debian.org  
debian.proxad.net  
ftp.ec-m.fr  
deb-mirr.naitways.net  
miroir.univ-lorraine.fr  
ftp.u-picardie.fr  
ftp.u-strasbg.fr  
mirror.plusserver.com  
debian.mirror.ate.info  
debian.univ-tlse2.fr  
ftp.rezopole.net  
ftp.univ-pau.fr  
mirrors.ircam.fr  
ftp.lip6.fr  
debian.polytech-lille.fr  
debian.apt-mirror.de  
debian.obspm.fr  
mirror.johnnybegood.fr  
apt.tetaneutral.net  
debian-archive.trafficmanager.net

[<Revenir en arrière>](#)

faite « continuer » :

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

Les paramètres du mandataire doivent être indiqués avec la forme normalisée « http://[[utilisateur][:mot-de-passe]@]hôte[:port]/ ».

Mandataire HTTP (laisser vide si aucun) :

<Revenir en arrière> <Continuer>

Cliquer sur « non » :

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 choisissez 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 ?

<Revenir en arrière> <Oui> <Non>

Decocher puis faire « continuer » :

Actuellement, seul le système de base est installé. Pour adapter l'installation à vos besoins, vous pouvez choisir d'installer un ou plusieurs ensembles prédéfinis de logiciels.

Logiciels à installer :

[ ] environnement de bureau Debian  
[\*] ... GNOME  
[ ] ... Xfce  
[ ] ... bureau GNOME Flashback  
[ ] ... KDE Plasma  
[ ] ... Cinnamon  
[ ] ... MATE  
[ ] ... LXDE  
[ ] ... LXQt  
[ ] serveur web  
[ ] serveur SSH  
[\*] utilitaires usuels du système

<Continuer>

Faire « oui » :

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 d'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 ?

<Revenir en arrière> <Oui> <Non>

Choisir la première option :

Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode habituelle pour cela est de l'installer sur le disque principal (partition UEFI ou secteur d'amorçage). Vous pouvez, si vous le souhaitez, l'installer ailleurs sur un autre disque, une autre partition, ou même sur un support amovible.

Périphérique où sera installé le programme de démarrage :

Choix manuel du périphérique  
/dev/sda (ata-QEMU\_HARDDISK\_0M00005)

<Revenir en arrière>

Faire « continuer » :

Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode habituelle pour cela est de l'installer sur le disque principal (partition UEFI ou secteur d'amorçage). Vous pouvez, si vous le souhaitez, l'installer ailleurs sur un autre disque, une autre partition, ou même sur un support amovible.

Le périphérique doit être indiqué avec un nom d'un périphérique dans /dev. Quelques exemples :

- « /dev/sda » utilisera le disque principal (partition UEFI ou secteur d'amorçage) ;
- « /dev/sdb » utilisera un disque secondaire (qui peut être amovible) ;
- « /dev/fd0 » installera GRUB sur une disquette.

Périphérique où sera installé le programme de démarrage :

[« Revenir en arrière »](#)

[« Continuer »](#)

l'installation est maintenant terminé  
faite « continuer » :

#### Installation terminée

L'installation est terminée et vous allez pouvoir maintenant démarrer le nouveau système. Veuillez vérifier que le support d'installation est bien retiré afin que le nouveau système puisse démarrer et éviter de relancer la procédure d'installation.

Veuillez sélectionner <Continuer> pour redémarrer.

[« Revenir en arrière »](#)

[« Continuer »](#)

On se connecte ensuite en « root » pour avoir tout les droits et accès :

```
On [?] login as: zabbix
[?] zabbix@192.168.10.5's password:
Linux zabbix 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
zabbix@zabbix:~$ su -
```

regarde les mise a jour en cours et a faire :

```
root@zabbix:~# apt update && apt upgrade -y
Atteint :1 http://security.debian.org/debian-security bookworm-security InRelease
Atteint :2 http://deb.debian.org/debian bookworm InRelease
Atteint :3 http://deb.debian.org/debian bookworm-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

On installe **wget** (téléchargement de fichiers) et **gnupg2** (gestion des clés GPG) avec confirmation automatique :

```
root@zabbix:~# apt install -y wget gnupg2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
wget est déjà la version la plus récente (1.21.3-1+b2).
gnupg2 est déjà la version la plus récente (2.2.40-1.1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

On télécharge un fichier depuis le dépôt officiel de Zabbix (par exemple, un paquet .deb pour l'installation du client ou du serveur Zabbix).

```
root@zabbix:~# wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb  
root@zabbix:~# sudo dpkg -i zabbix-release_5.0-1+focal_all.deb  
root@zabbix:~# --2024-10-17 11:56:48-- https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb  
root@zabbix:~# Résolution de repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:  
root@zabbix:~#
```

faite « N » :

```
root@zabbix:~# dpkg -i zabbix-release_latest+debian12_all.deb
Lecture de la base de données... 34362 fichiers et répertoires déjà installés.)
réparation du dépaquetage de zabbix-release_latest+debian12_all.deb ...
épaquetage de zabbix-release (1:7.0-2+debian12) sur (1:5.0-1+focal) ...
aramétrage de zabbix-release (1:7.0-2+debian12) ...

Fichier de configuration « /etc/apt/sources.list.d/zabbix.list »
==> Modifié (par vous ou par un script) depuis l'installation.
==> Le distributeur du paquet a fourni une version mise à jour.
Que voulez-vous faire ? Vos options sont les suivantes :
 Y ou I : installer la version du responsable du paquet
 N ou O : garder votre version actuellement installée
 D : afficher les différences entre les versions
 Z : suspendre ce processus pour examiner la situation
L'action par défaut garde votre version actuelle.
** zabbix.list (Y/I/N/O/D/Z) [défaut=N] ? N
nstallation de la nouvelle version du fichier de configuration /etc/apt/trusted
gpg.d/zabbix-official-repo.gpg ...
```

On installe tous les composants nécessaires à un serveur Zabbix complet : serveur Zabbix avec MySQL, interface web en PHP, configuration Apache, scripts SQL pour la base de données, et l'agent pour la supervision locale :

```
root@zabbix:~# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-co
nf zabbix-sql-scripts zabbix-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
zabbix-server-mysql est déjà la version la plus récente (1:7.0.5-1+debian12).
zabbix-frontend-php est déjà la version la plus récente (1:7.0.5-1+debian12).
zabbix-agent est déjà la version la plus récente (1:7.0.5-1+debian12).
Les NOUVEAUX paquets suivants seront installés :
  zabbix-apache-conf zabbix-sql-scripts
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 9037 ko dans les archives.
Après cette opération, 10,1 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

La commande permet de se connecter à MySQL en tant qu'utilisateur **root**. Le **-p** indique qu'il faut entrer un mot de passe pour l'utilisateur root. Lorsque vous appuyez sur Entrée, il vous sera demandé de saisir le mot de passe de l'utilisateur root de MySQL :

```
root@zabbix:~# mysql -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

décomprime et importe le fichier SQL de Zabbix dans la base de données zabbix en utilisant l'utilisateur zabbix

```
root@zabbix:~# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:
```

Dans Zabbix, **MariaDB** sert de système de gestion de base de données pour stocker les données de supervision (performances, alertes, historiques) et la configuration (utilisateurs, hôtes, déclencheurs). Il permet de gérer efficacement de grandes quantités de données, avec des fonctionnalités de recherche et d'indexation pour optimiser les requêtes. Lors de l'installation, MariaDB est configurée pour créer les tables et schémas nécessaires à Zabbix.

```
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 46
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> set global log_bin_trust_function_creators = 0;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> quit;
Bye
```

On redémarre les services **zabbix-server**, **zabbix-agent** et **apache2** pour appliquer les modifications de configuration et garantir que les services fonctionnent correctement après les changements.

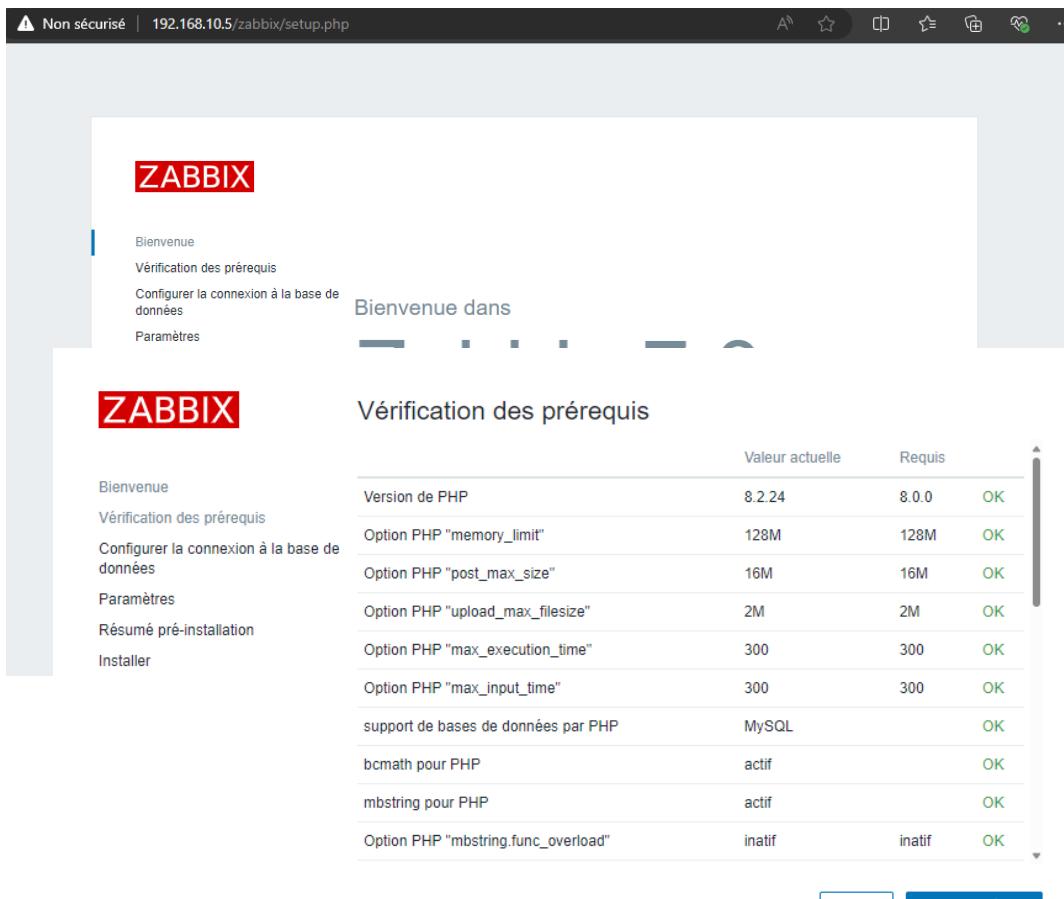
On active les services **zabbix-server**, **zabbix-agent** et **apache2** pour qu'ils démarrent automatiquement au démarrage du système. Cela assure que ces services sont toujours en fonctionnement après un redémarrage du serveur.

```
root@zabbix:~# DBPassword=password
root@zabbix:~# systemctl restart zabbix-server zabbix-agent apache2
root@zabbix:~# systemctl enable zabbix-server zabbix-agent apache2
```

ouvez votre navigateur et entrez l'adresse IP de votre serveur Web plus /zabbix.

Dans notre exemple, l'URL suivante a été saisie dans le navigateur :

<http://192.168.10.5/zabbix>

sur  Cliquer

« prochaine étape » :

« prochaine étape » :

ZABBIX

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Bienvenue dans

ZABBIX

Vérification des prérequis

	Valeur actuelle	Requis	
Version de PHP	8.2.24	8.0.0	OK
Option PHP "memory_limit"	128M	128M	OK
Option PHP "post_max_size"	16M	16M	OK
Option PHP "upload_max_filesize"	2M	2M	OK
Option PHP "max_execution_time"	300	300	OK
Option PHP "max_input_time"	300	300	OK
support de bases de données par PHP	MySQL		OK
bcmath pour PHP	actif		OK
mbstring pour PHP	actif		OK
Option PHP "mbstring.func_overload"	inatif		OK

Retour

Prochaine étape

## ZABBIX

### Configurer la connexion à la base de données

Veuillez créer la base de données manuellement et configurer les paramètres de connexion. Appuyez sur le bouton "Prochaine étape" quand c'est fait.

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Résumé pré-installation

Installer

Type de base de données

Hôte base de données

Port de la base de données  0 - utiliser le port par défaut

Nom de la base de données

Stocker les informations d'identification dans  Texte brut  Coffre HashiCorp  Coffre CyberArk

Utilisateur

Mot de passe

Chiffrement TLS de la base de données *La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix) ou de la mémoire partagée (Windows).*

[Retour](#)

[Prochaine étape](#)

donner un nom au serveur puis continuer :

## ZABBIX

### Paramètres

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Résumé pré-installation

Installer

Nom du serveur Zabbix

Fuseau horaire par défaut

Thème par défaut

[Retour](#)

[Prochaine étape](#)

L'installation est terminé cliquer sur « terminé » :



Installer

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Résumé pré-installation

Installer

**Félicitations ! Vous avez installé l'interface Zabbix avec succès.**

Fichier de configuration "conf/zabbix.conf.php" créé.

[Retour](#)

[Terminé](#)

Sur l'écran de connexion, utilisez le nom d'utilisateur par défaut et le mot de passe par défaut.

- Default Username: Admin
- Default Password: zabbix



Nom d'utilisateur

Admin

Mot de passe

.....

Me rappeler toutes les 30 jours

**S'enregistrer**

Configurer la supervision des services

Configurer le serveur de messagerie dans Zabbix ( SMTP )

Sur l'écran du tableau de bord, accédez au menu Administration et sélectionnez l'option Types de médias.

Localisez et cliquez sur l'option nommée Email.

The screenshot shows the Zabbix Administration interface with the 'Email (HTML)' configuration page. At the top, there are tabs for 'Email (HTML)', 'Courriel' (selected), and 'Activé'. A status bar at the top right indicates: 'Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers' and 'serveur SMTP: "mail.example.com", SMTP helo: "example.courriel: "zabbix@example.com"".

Dans l'écran Propriétés de l'e-mail, vous devez entrer la configuration suivante.

The screenshot shows the 'Type de média' configuration form for 'Email (HTML)'. The form includes fields for Name (Nom), Type (Courriel), Provider (Fournisseur de messagerie), SMTP server (serveur SMTP), Port (Port du serveur SMTP), From email (Courriel), SMTP helo (SMTP helo), Security (Sécurité de la connexion), SSL verification (Vérifier le pair SSL), Host verification (Vérifier l'hôte SSL), Authentication (Authentification), User (Nom d'utilisateur), Password (Mot de passe), Message format (Format du message), and a Description area. The 'STARTTLS' tab is selected under security. The 'Actualiser' button is visible at the bottom right.

Type de média

Nom: Email (HTML)

Type: Courriel

Fournisseur de messagerie: Generic SMTP

serveur SMTP: mail.example.com

Port du serveur SMTP: 587

Courriel: mariam.asseas@btssio.dedyn.io

SMTP helo: example.com

Sécurité de la connexion: STARTTLS

Vérifier le pair SSL:

Vérifier l'hôte SSL:

Authentification: Nom d'utilisateur et mot de passe

Nom d'utilisateur: mariam.asseas@btssio.dedyn.io

Mot de passe:

Format du message: HTML

Description:

Activé:

Actualiser, Clone, Supprimer, Annuler

Cliquez sur le bouton Mise à jour.

Recherchez et l'option nommée : Signaler les problèmes aux administrateurs Zabbix  
Pour activer cette action, vous devez cliquer sur le mot Désactivé en rouge.

Cela configurera Zabbi pour envoyer des notifications par courrier électronique aux utilisateurs membres du groupe Administrateur Zabbix.

Nom	Conditions	Opérations	État
Report problems to Zabbix administrators	Envoyer le message aux groupes d'utilisateurs: Zabbix administrators via tous les médias		Activé

Affichage de 1 sur 1 trouvés

Par défaut, seul l'utilisateur Admin est membre du groupe Administrateurs Zabbix.

Par défaut, l'utilisateur Admin n'a pas d'adresse e-mail associée au compte.

Maintenant, nous devons associer une adresse e-mail au compte Admin.

Connectez-vous sur l'interface Web zabbix en tant qu'utilisateur Admin.

Dans la partie en bas à gauche de l'écran, accédez aux paramètres du profil utilisateur.

Sur l'écran du profil utilisateur, accédez à l'onglet Média et ajoutez une nouvelle configuration de messagerie.

Ajouter votre

Profil utilisateur: Zabbix Administrator

**Média**

Média	Type	Envoyer à	Lorsque actif	Utiliser si严重度	État	Action
Email (HTML)	mariam.asseas@btssio.dedyn.io	1-7,00:00-24:00	<input checked="" type="checkbox"/> Non classé <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Avertissement <input checked="" type="checkbox"/> Moyen <input checked="" type="checkbox"/> Haut <input checked="" type="checkbox"/> Désastre	<input checked="" type="checkbox"/>	Activé	<a href="#">Ajouter</a> <a href="#">Annuler</a>

adresse :

Média	Type	Envoyer à	Lorsque actif	Utiliser si严重度	État	Action
Email (HTML)	mariam.asseas@btssio.dedyn.io	1-7,00:00-24:00	<input checked="" type="checkbox"/> N <input checked="" type="checkbox"/> I <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> M <input checked="" type="checkbox"/> H <input checked="" type="checkbox"/> D	Activé	<a href="#">Édition</a> <a href="#">Supprimer</a>	

[Actualiser](#) [Annuler](#)

vous avez configuré la notification par e-mail du serveur Zabbix

## Installation de l'agent sur Windows

Pour pouvoir installer un agent on se connecte sur le windows serveur

Puis on récupère la dernière version de l'agent pour cela on se rend sur le site officiel de zabbix

### Zabbix agent 2 v7.0.5

[Read manual](#)

Packaging: MSI

Encryption: OpenSSL

Linkage: Dynamic

Checksum: sha256: 4a9601b5e74d7cab6257dc520fd715366ae63342261dae9a253bc2ba0a4afa10

sha1: 8a28a04f6118b7acceaedd40eaa8f8e64b61501a

md5: bd2a1b91d0cac9037813a52d4e5d3858

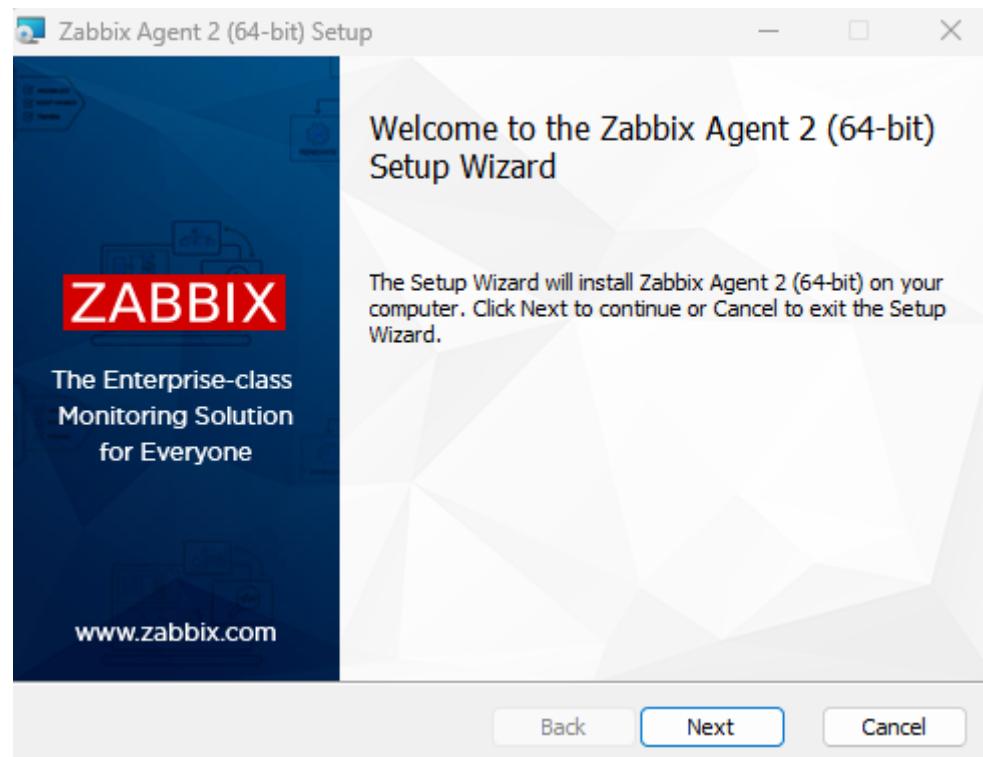
[DOWNLOAD](#)

[https://cdn.zabbix.com/zabbix/binaries/stable/7.0/7.0.5/zabbix\\_agent2-7.0.5-](https://cdn.zabbix.com/zabbix/binaries/stable/7.0/7.0.5/zabbix_agent2-7.0.5-windows-amd64-openssl.msi)

windows-amd64-openssl.msi

Exécutez l'agent ensuite en ajoutant toutes les fonctionnalités souhaitées.

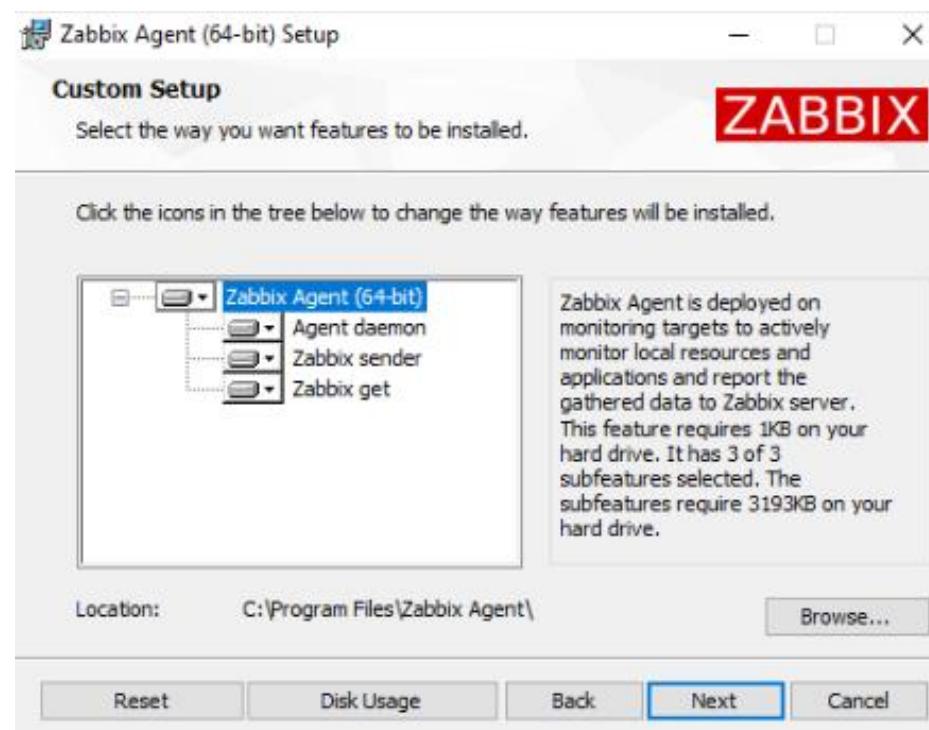
Ensuite, renseignez le nom d'hôte du serveur à surveiller, ainsi que les détails du serveur Zabbix, en indiquant le port, qui est par défaut 10050.



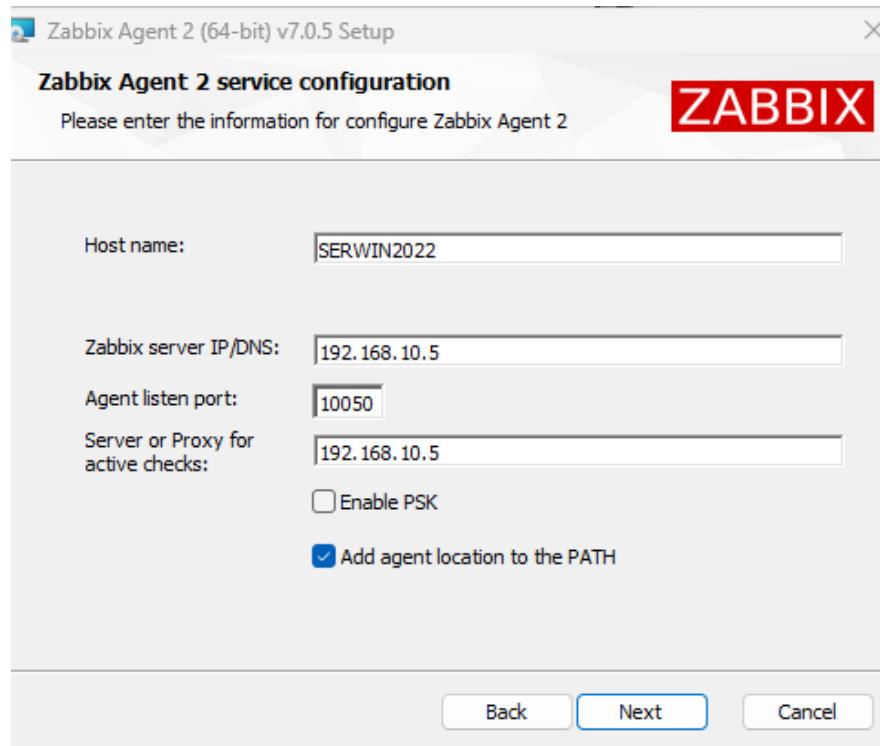
Fait « next » :  
Puis cocher en bas a droite



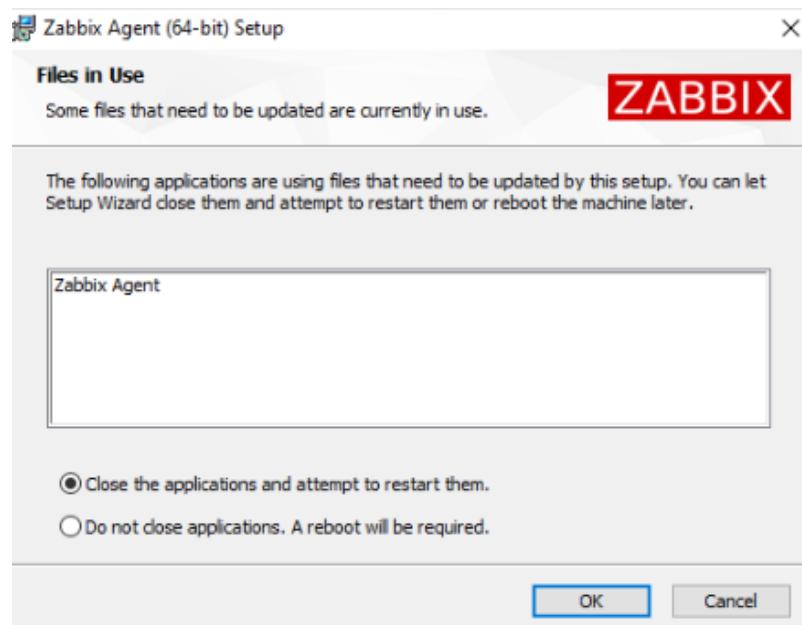
Fait  
« next » :



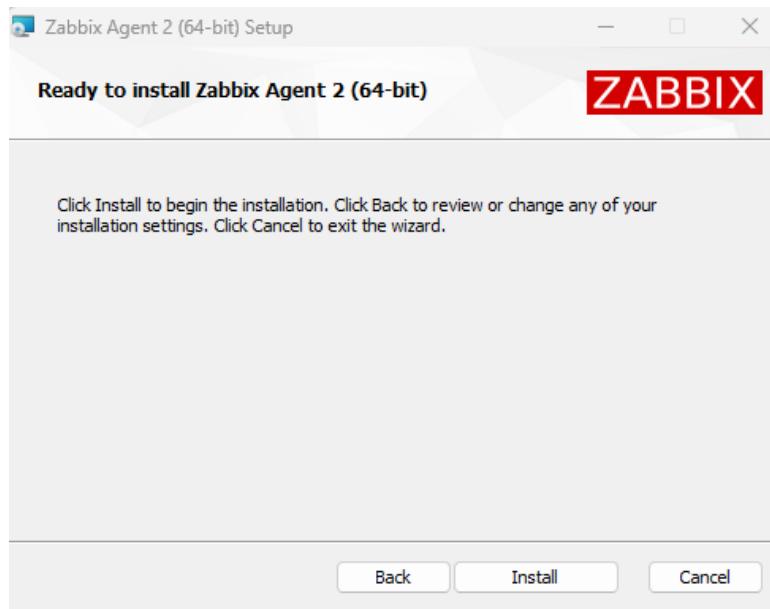
ajouter le nom de l'agent  
puis ajouter l'adresse IP du serveur zabbix  
Puis cocher la case en bas



Fait «ok» :



Cliquer sur « install » :



Ensuite, pour ajouter l'hôte dans Zabbix, allez dans l'onglet « Collecte de données », puis sélectionnez « Hôtes ». Cliquez sur « Créer un hôte » en haut à droite pour commencer la configuration.

Indiquez le nom que vous souhaitez voir apparaître pour l'hôte  
sélectionnez le modèle « Windows by Zabbix agent »  
choisissez le groupe d'hôte que vous souhaitez  
configurez l'interface en précisant soit le DNS, soit l'IP de l'hôte, avec le port 10050 utilisé par l'agent Zabbix.  
( ajouter l'adresse ip de l'agent en question )

Nouvel hôte

Hôte	IPMI	Tags	Macros	Inventaire	Chiffrement	Table de correspondance
* Nom de l'hôte WINSERV2022						
Nom visible WINSERV2022						
Modèles Windows by Zabbix agent	Sélectionner					
taper ici pour rechercher						
* Groupes d'hôtes Virtual machines	Sélectionner					
taper ici pour rechercher						
Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	IP	192.168.10.5		DNS	10050	Supprimer
<a href="#">Ajouter</a>						
Description						
Surveillé par	Serveur	Proxy	Groupe de proxy			
Activé	<input checked="" type="checkbox"/>					

On suit les mêmes étapes précédentes pour toute nos machine windows :

En l'occurrence le client Windows :  
 ( ajouter l'adresse ip de l'agent en question )

Nouvel hôte

On  
vas

Hôte	IPMI	Tags	Macros	Inventaire	Chiffrement	Table de correspondance
* Nom de l'hôte	CLIENTWIN10					
Nom visible	CLIENTWIN10					
Modèles	Windows by Zabbix agent <span style="color: red;">X</span>			<a href="#">Sélectionner</a>		
* Groupes d'hôtes	Virtual machines <span style="color: red;">X</span>			<a href="#">Sélectionner</a>		
Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
	Agent	192.168.10.5		<a href="#">IP</a>	<a href="#">DNS</a>	<a href="#">10050</a>
<a href="#">Ajouter</a>						
Description	<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>					
Surveillé par	<a href="#">Serveur</a> <a href="#">Proxy</a> <a href="#">Groupe de proxy</a>					
Activé	<input checked="" type="checkbox"/>					

maintenant installer les agents sur les machine linux :

Ajoutez des dépôts Zabbix à l'aide des commandes ci-dessous :

installe Zabbix Agent, qui envoie des données système au serveur Zabbix.

```
root@serveurweb:~# apt install zabbix-agent
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 :
 libmodbus5
Les NOUVEAUX paquets suivants seront installés :
 libmodbus5 zabbix-agent
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 706 ko dans les archives.
Après cette opération, 1 504 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libmodbus5 amd64 3.1.6-2.1 [31,3 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 zabbix-agent amd64 1:6.0.14+dfsg-1+b1 [675 kB]
706 ko réceptionnés en 10s (69,4 ko/s)
Sélection du paquet libmodbus5:amd64 précédemment désélectionné.
(Lecture de la base de données... 35154 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libmodbus5_3.1.6-2.1_amd64.deb ...
Dépaquetage de libmodbus5:amd64 (3.1.6-2.1) ...
Sélection du paquet zabbix-agent précédemment désélectionné.
Préparation du dépaquetage de .../zabbix-agent_1%3a6.0.14+dfsg-1+b1_amd64.deb ...
Dépaquetage de zabbix-agent (1:6.0.14+dfsg-1+b1) ...
Paramétrage de libmodbus5:amd64 (3.1.6-2.1) ...
Paramétrage de zabbix-agent (1:6.0.14+dfsg-1+b1) ...

Creating config file /etc/zabbix/zabbix_agentd.conf with new version
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
Traitement des actions différencées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différencées (« triggers ») pour libc-bin (2.36-9+deb12u8) ...
```

La commande nano /etc/zabbix/zabbix\_agentd.conf permet de configurer Zabbix Agent (adresse du serveur avec Server=..., nom de l'agent avec Hostname=...) :

```
root@serveurweb:~# nano /etc/zabbix/zabbix_agentd.conf
```

On ajoute l'adresse ip du serveur zabbix :

ici

```
# Mandatory: yes, if startArgments is not explicitly set to 0
# Default:
# Server=

Server=192.168.10.5

### Option: ListenPort
#           Agent will listen on this port for connections from the server.
#
```

également :

```
# Mandatory: no
# Default:
# ServerActive=

ServerActive=192.168.10.5

### Option: Hostname
#           List of comma delimited unique, case sensitive hostnames.
#           Required for active checks and must match hostnames as configured on the server.
#           Value is acquired from HostnameItem if undefined.
#
```

Après modification, redémarrez l'agent :

```
root@serveurweb:~# systemctl restart zabbix-agent
root@serveurweb:~# systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-11-21 09:59:43 CET; 18s ago
     Docs: man:zabbix_agentd(8)
   Main PID: 1070 (zabbix_agentd)
      Tasks: 6 (limit: 2305)
     Memory: 2.7M
        CPU: 25ms
      CGroup: /system.slice/zabbix-agent.service
              └─1070 /usr/sbin/zabbix_agentd --foreground
                  ├─1072 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]"
                  ├─1073 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
                  ├─1074 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
                  ├─1075 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"
                  └─1076 "/usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]"

nov. 21 09:59:43 serveurweb systemd[1]: Started zabbix-agent.service - Zabbix Agent.
nov. 21 09:59:43 serveurweb zabbix_agentd[1070]: Starting Zabbix Agent [serveurweb]. Zabbix 6.0.14 (revision 3f184b456c7).
nov. 21 09:59:43 serveurweb zabbix_agentd[1070]: Press Ctrl+C to exit.
```

cliquer sur « créer un hôte » en haut a droite :

?      **Créer un hôte**

( ajouter l'adresse ip de l'agent en question )

## Nouvel hôte

Hôte    IPMI    Tags    Macros    Inventaire    Chiffrement    Table de correspondance

\* Nom de l'hôte : SERVWEB  
Nom visible : SERVWEB  
Modèles : Linux by Zabbix agent     
taper ici pour rechercher

\* Groupes d'hôtes : Virtual machines     
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	
	Agent	192.168.10.5		IP	DNS	10050

[Ajouter](#)

Description :

Surveillé par :  Serveur    Proxy    Groupe de proxy

On le meme processus pour le serveur frais :  
( ajouter l'adresse ip de l'agent en question )

## Nouvel hôte

Nous

Hôte    IPMI    Tags    Macros    Inventaire    Chiffrement    Table de correspondance

\* Nom de l'hôte : SERVFRAIS  
Nom visible : SERVFRAIS  
Modèles : Linux by Zabbix agent     
taper ici pour rechercher

\* Groupes d'hôtes : Virtual machines     
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	
	Agent	192.168.10.5		IP	DNS	10050

[Ajouter](#)

Description :

Surveillé par :  Serveur    Proxy    Groupe de proxy

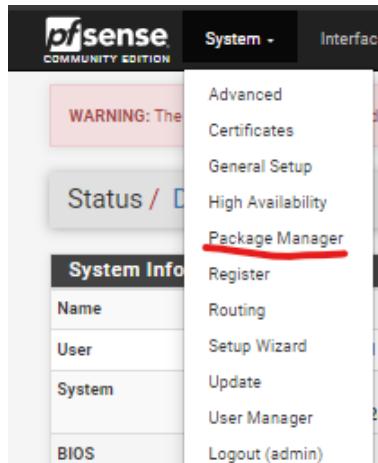
Activé

allons maintenant installé l'agent zabbix

Ouvrez un logiciel de navigateur, entrez l'adresse IP de votre pare-feu PfSense et accédez à l'interface Web.

Après une connexion réussie, vous serez envoyé au tableau de bord PfSense.

Accédez au menu Pfsense System et sélectionnez l'option De gestionnaire de paquets.



Sur l'écran du gestionnaire de paquets, accédez à l'onglet Paquets disponibles.

Sous l'onglet Packages disponibles, recherchez zabbix-agent et installez le package de l'agent Zabbix.

A screenshot of the 'Available Packages' tab in the Pfsense Package Manager. The title bar says 'System / Package Manager / Available Packages'. Below it, there are two tabs: 'Installed Packages' (disabled) and 'Available Packages' (selected, indicated by a red underline). A search bar at the top has 'zabbix-agent' entered. A note below the search bar says 'Enter a search string or \*nix regular expression to search package names and descriptions.'

A screenshot of the search results for 'zabbix-agent'. The search bar shows 'zabbix-agent'. A note below it says 'Enter a search string or \*nix regular expression to search package names and descriptions.'. The results table shows one entry: 'zabbix-proxy64 1.0.6'. The description states: 'A Zabbix proxy can collect performance and availability data on behalf of the Zabbix server. This way, a proxy can take on itself some of the load of collecting data and offload the Zabbix server. Also, using a proxy is the easiest way of implementing centralized and distributed monitoring, when all agents and proxies report to one Zabbix server and all data is collected centrally. Zabbix is an enterprise-class open source distributed monitoring solution.' Below the description, it says 'Package Dependencies: zabbix64-proxy-6.4.7'. On the right, there is a green 'Install' button with a plus sign.

Attendez la fin de l'installation de l'agent Zabbix.

Accédez au menu Pfsense Services et sélectionnez l'option Zabbix Agent.



Sous l'onglet Général, activez le service d'agent Zabbix et effectuez la configuration suivante :

Serveur – L'adresse IP du serveur Zabbix

ServerActive – L'adresse IP du serveur Zabbix

Hostname – Le nom d'hôte du pare-feu PFsense

Écouter IP – Utilisez 0.0.0.0 pour écouter sur toutes les adresses IP

Écouter Port – Zabbix agent par défaut port 10050

**Zabbix Agent Settings**

Enable	<input checked="" type="checkbox"/> Enable Zabbix Agent service.
Server	192.168.10.5 List of comma delimited IP addresses (or hostnames) of ZABBIX servers.
Server Active	192.168.10.5 List of comma delimited IP:port (or hostname:port) pairs of Zabbix servers for active checks.
Hostname	PFSENSE-FIREWALL Unique, case sensitive hostname. Required for active checks and must match hostname as configured on the Zabbix server.
Listen IP	0.0.0.0 Comma-separated list of IP addresses for connections from the server. (Default: 0.0.0.0 - all IPv4 interfaces)
Listen Port	10050 Listen port for connections from the server. (Default: 10050)
Refresh Active Checks	120 The agent will refresh list of active checks once per this number of seconds. (Default: 120)
Timeout	3 Do not spend more than N seconds on getting requested value. Note: The agent does not kill timeouted User Parameters processes! (Default: 3. Valid range: 1-30)
Buffer Send	5 Do not keep data longer than N seconds in buffer. (Default: 5. Valid range: 1-3600)
Buffer Size	100 Maximum number of values in the memory buffer. The agent will send all collected data to Zabbix server or proxy if the buffer is full. (Default: 100. Valid range: 2-65535)

Le serveur Zabbix a l'adresse IP: 192.168.15.10.

Le nom d'hôte du pare-feu Pfsense est : PFSENSE-FIREWALL

La clé d'identification PSK a été nommée : key-pfsense-01

La communication sera chiffrée à l'aide de la clé suivante :

fb6616cd582a2fa0aa161cab3423a9ca640c931b21c8c2e3b7132d6db75aadff

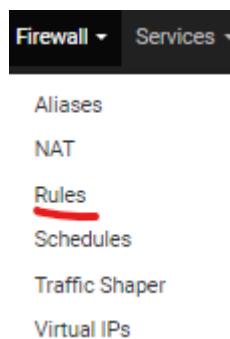
Vous avez installé avec succès l'agent Pfsense Zabbix.

Après avoir terminé la configuration, cliquez sur le bouton Enregistrer dans la partie inférieure de l'écran

Par défaut, le pare-feu Pfsense n'autorise pas les connexions Zabbix externes à l'interface WAN.

Nous allons créer une règle de pare-feu pour autoriser la communication Zabbix.

Accédez au menu Pare-feu Pfsense et sélectionnez l'option Règles.



Cliquez sur le bouton Ajouter pour ajouter une règle au haut de la liste.

Floating   WAN   LAN   DMZ   WIFI

### Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/630 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/3 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface  
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add   Add   Delete   Toggle   Copy   Save   Separator

Sur l'écran De configuration source, vous devez définir l'adresse IP du serveur Zabbix.

Cette adresse IP doit être autorisée à communiquer avec l'agent Zabbix installé sur le pare-feu Pfsense.

Ici seul l'ordinateur utilisant l'adresse IP 192.168.10, pourra communiquer avec l'agent Pfsense Zabbix.

Sur l'écran de destination Firewall, effectuez la configuration suivante :

Destination – Adresse Wan

Plage de ports de destination – De (Autre) 10050 à (Autre) 10050

### Source

<u>Source</u>	<input type="checkbox"/> Invert match	Address or Alias	192.168.10.5
---------------	---------------------------------------	------------------	--------------

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

### Destination

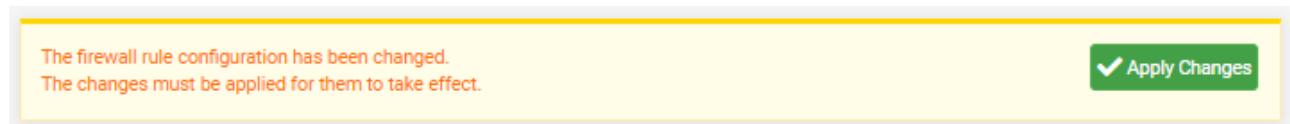
<u>Destination</u>	<input type="checkbox"/> Invert match	WAN address	Destination Address	
Destination Port Range	(other)	10050	(other)	10050
From	Custom	To	Custom	

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

### Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the <a href="#">Status: System Logs: Settings page</a> ).	
Description	<input type="text"/>
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	

Vous avez terminé la configuration du pare-feu PFsense pour permettre la communication du serveur Zabbix à l'aide de l'interface WAN.



Maintenant, nous devons accéder au tableau de bord du serveur Zabbix et ajouter le serveur PfSense en tant qu'hôte.

En haut à droite de l'écran, cliquez sur le bouton Créez l'hôte.



Sur l'écran de configuration de l'hôte, vous devrez saisir les informations suivantes :

The screenshot shows the "Hôte" (Host) creation form in the Zabbix interface. The host name is set to "pfSense". It is associated with the "Virtual machines" group. An interface is defined with IP 192.168.10.1. The host is marked as active. The "Surveillé par" (Monitored by) section is set to "Serveur".

Hôte													
	Zabbix une												
Hôte	<input type="text" value="pfSense"/>												
IPMI													
Tags													
Macros													
Inventaire													
Chiffrement													
Table de correspondance													
* Nom de l'hôte	<input type="text" value="pfSense"/>												
Nom visible	<input type="text" value="pfSense"/>												
Modèles	<table><thead><tr><th>Nom</th><th>Action</th></tr></thead><tbody><tr><td>Linux by Zabbix agent</td><td><a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a></td></tr></tbody></table>	Nom	Action	Linux by Zabbix agent	<a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a>								
Nom	Action												
Linux by Zabbix agent	<a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a>												
	<input type="text" value="taper ici pour rechercher"/> <a href="#">Sélectionner</a>												
* Groupes d'hôtes	<table><thead><tr><th>Virtual machines</th><th>X</th><th>taper ici pour rechercher</th><th><a href="#">Sélectionner</a></th></tr></thead></table>	Virtual machines	X	taper ici pour rechercher	<a href="#">Sélectionner</a>								
Virtual machines	X	taper ici pour rechercher	<a href="#">Sélectionner</a>										
Interfaces	<table><thead><tr><th>Type</th><th>adresse IP</th><th>Nom DNS</th><th>Connexion à</th><th>Port</th><th>Défaut</th></tr></thead><tbody><tr><td>Agent</td><td><input type="text" value="192.168.10.1"/></td><td><input type="text"/></td><td><input type="radio"/> IP</td><td><input type="radio"/> DNS</td><td><input type="radio"/> 10050</td></tr></tbody></table>	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut	Agent	<input type="text" value="192.168.10.1"/>	<input type="text"/>	<input type="radio"/> IP	<input type="radio"/> DNS	<input type="radio"/> 10050
Type	adresse IP	Nom DNS	Connexion à	Port	Défaut								
Agent	<input type="text" value="192.168.10.1"/>	<input type="text"/>	<input type="radio"/> IP	<input type="radio"/> DNS	<input type="radio"/> 10050								
	<a href="#">Supprimer</a>												
	<a href="#">Ajouter</a>												
Description	<input type="text"/>												
Surveillé par	<input checked="" type="radio"/> Serveur <input type="radio"/> Proxy <input type="radio"/> Groupe de proxy												
Activé	<input checked="" type="checkbox"/>												

La solution de supervision Zabbix permet de surveiller en temps réel l'état des systèmes informatiques (serveurs, applications, réseaux). Il collecte des données, génère des alertes en cas de problème, et fournit des graphiques et rapports via l'interface web pour analyser les performances et prévenir les pannes.