



Projet BTS SIO Epreuve E5

Sommaire

Sommaire	2
Présentation	4
Contexte	4
Groupe	4
Matériel	4
Objectifs	5
1. Créer l'infrastructure réseau de l'entreprise.	5
2. Mise en place des serveurs nécessaires à l'entreprise.	5
3. Paramétrage des clients.	5
Spécifications	5
Infrastructure réseau	5
Réseau de Marseille	5
Infos	5
Connexion	6
Routeur	6
Switch	6
Schéma	6
Configuration des VLANs	6
Configuration du DHCP	7
Configuration du NAT	7
Règles de parefeu	8
Borne WI-FI	9
Infos	9
Accès	9
Réseau de Lille	9
Infos	9
Schéma	10
Configuration des VLAN	10
Configuration du DHCP	10
Configuration du NAT	10
Règles de parefeu	11
Schéma Général	11
VPN Site à Site	11
Tableau de synthèse des VMs et Conteneurs	12
WinServ1MarsAD: Service d'authentification	13
Infos	13
Utilisateurs et Groupes:	14
Partages SMB	14
Enregistrement DNS	15

GPOs	15
Serveur Radius & AD CS	16
DebSGBD1Mars: Base de donnée MySQL (avec PhpMyAdmin)	16
Infos	16
Accès Web	16
Présentation	16
Solution de sauvegarde	17
Fréquence	17
Gestion	17
DebGLPI1Mars: Gestion des incidents avec GLPI	18
Infos	18
Accès Web	18
Présentation de l'interface d'administration	18
Création d'un ticket de support	18
Gestion d'un élément du parc informatique	18
DebPki1Mars: La PKI	18
Infos	18
Autorité de certification	19
Fichiers	19
Utilisation	19
Supervision	19
DebZabbixMars: Services	19
Accès Web	19
Présentation	19
DebAlert1Mars: Réseau	22
Infos	22
Accès Web	22
Présentation	22
DebNginx1Mars: Equilibrage des charges	23
Infos	23
Présentation	23
Exemple de configuration (GLPI)	23
UbuWazuh1Mars:	23
Infos	23
Accès Web	23
Configuration	23
Log	24
Utilisation	24
DebSquid1Mars: Serveur Proxy	24
Infos	24
Configuration	24

Les réseaux autorisé	24
Marseille	24
Lille	25
Les ports autorisé	25
Les domaines bloqués sont:	25
Exemple	25
GPO	25
DebAnsible1Mars: Serveur Ansible	26
Infos	26
Configuration	26
Hôtes	27
Déploiements	27
Exemple	27
Annexe 10	29

Présentation

Contexte

Créée en 2005, ITWay a commencé comme une petite entreprise de conseil en informatique. Avec l'augmentation des besoins en services numériques et la complexification des infrastructures IT, l'entreprise a rapidement élargie ses activités pour offrir des services d'intégration, de maintenance de réseaux, de gestion des systèmes informatiques et de cybersécurité. En 2018, ITWay a ouvert une antenne régionale pour mieux desservir ses clients en France et à l'international.

Groupe

Les membres du projet sont les suivants :

- Octave LAPCHIN
- Tom BILBAULT

Matériel

Nous disposons de 2 switchs, un PoE et un non PoE, nous avons une borne Wi-Fi Aruba.

Nous avons un serveur HPE ILO 5 avec:

- CPU : Intel(R) Xeon(R) Gold 6148 2.40GHz
- RAM : 64 GB
- Disques : 4 de 1.2 TB et 2 de 600 GB

Objectifs

1. Créer l'infrastructure réseau de l'entreprise.

- 1.1 Création des VLAN
- 1.2 Création des POOL DHCP
- 1.3 Création des règles de parefeu

2. Mise en place des serveurs nécessaires à l'entreprise.

3. Paramétrage des clients.

Spécifications

L'infrastructure doit comporter deux routeurs, un physique (Cisco) et un virtuel (PfSense), deux switchs (un PoE et un non PoE), ainsi qu'une borne WI-FI. Il doit également y avoir les services suivants: un service d'authentification (AD-DS), un SGBD (MySQL), un accès à internet (pour les clients), un environnement de travail collaboratif (Office 365, Discord, Notion), deux systèmes d'exploitations pour les serveurs (Linux et Windows). Une solution de sauvegarde, des ressources avec accès sécurisés et soumis à un contrôle d'accès, un serveur GLPI, il faut Fail2ban sur les serveurs linux, une PKI qui fournira les certificats SSL à tous les serveurs WEB. Sécurisation avec des ACL, et règles de parefeu. Un serveur de supervision (Zabbix), wireshark doit être présent sur toutes les VM, les agents GLPI, ainsi qu'un autre de supervision réseau (PiAlert), une DMZ, une haute disponibilité grâce à la redondance, un TSE (Nginx), un VPN site à site.

Infrastructure réseau

Réseau de Marseille

Infos

Routeur Cisco 1841

Version: 12.4

Nous avons également une VM PfSense, avec la même configuration permettant une redondance du routeur de Marseille (RT-MRS-02).

Connexion

Routeur

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa  
-oMACs=+hmac-sha1 -c 3des-cbc ssh@192.168.150.54
```

Mot de passe ssh: **123456**

Mot de passe enable: **Passw0rd84!**

Switch

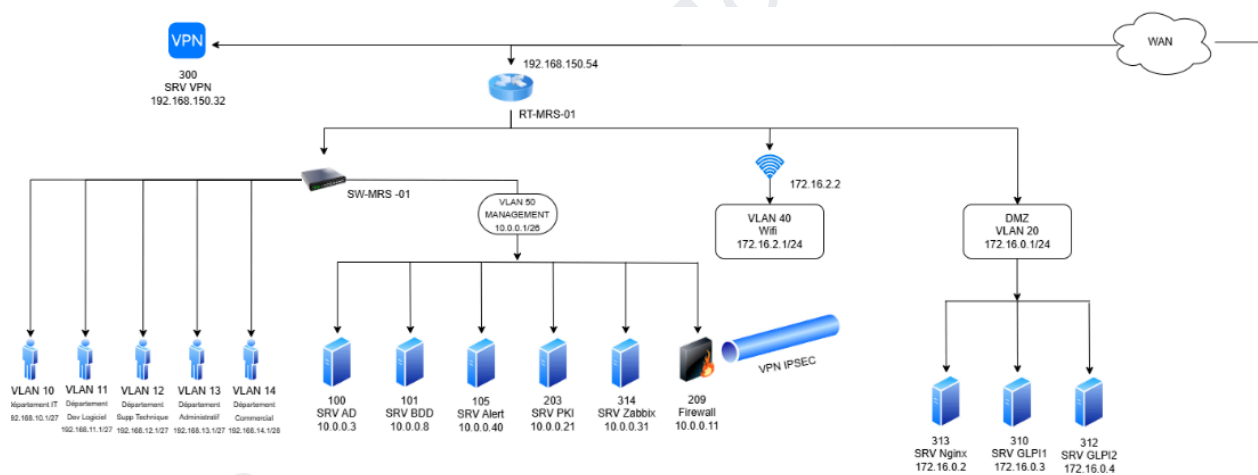
La connexion se fait par câble console avec les identifiants suivants.

Il est peut être nécessaire d'installer le driver du câble console sous windows.

Identifiant: **tomoctave**

Mot de passe: **3[6^)^69#Got***

Schéma



Configuration des VLANs

- VLAN 10 : Département IT → 192.168.10.1/27 (30 IP)
- VLAN 11 : Département Dev Logiciel → 192.168.11.1/27 (30 IP)
- VLAN 12 : Département Supp Technique → 192.168.12.1/27 (30 IP)
- VLAN 13 : Département Administratif → 192.168.13.1/27 (30 IP)
- VLAN 14 : Département Commercial → 192.168.14.1/28 (14 IP)
- VLAN 20 : DMZ → 172.16.0.1/24 (254 IP)
- VLAN 40 : Wifi → 172.16.2.1/24 (254 IP)
- VLAN 50 : MANAGEMENT → serveur 10.0.0.1/26 (63 IP)

Configuration du DHCP

VLAN	IP début	IP Fin	DNS	Passerelle	CIDR
10	192.168.10.2	192.168.10.30	10.0.0.3 172.16.3.4	192.168.10.1	192.168.10.1/27
11	192.168.11.2	192.168.11.30	10.0.0.3 172.16.3.4	192.168.11.1	192.168.11.1/27
12	192.168.12.2	192.168.12.30	10.0.0.3 172.16.3.4	192.168.12.1	192.168.12.1/27
13	192.168.13.2	192.168.13.30	10.0.0.3 172.16.3.4	192.168.13.1	192.168.13.1/27
14	192.168.14.2	192.168.14.30	10.0.0.3 172.16.3.4	192.168.14.1	192.168.14.1/27
20	172.16.0.2	172.16.0.254	10.0.0.3 172.16.3.4	172.16.0.1	172.16.0.1/24
40	172.16.2.3	172.16.2.254	10.0.0.3 172.16.3.4	172.16.2.1	172.16.2.1/24
50	10.0.0.2	10.0.0.62	10.0.0.3 172.16.3.4	10.0.0.1	10.0.0.1/26

Configuration du NAT

On autorise tous les VLAN à sortir vers le WAN.

Il y a deux règles qui NAT deux ports vers l'intérieur du VLAN 50:

- 192.168.150.54:3389 WAN (RDP) -> 10.0.0.4:3389 VLAN Serveur (RDP)
- 192.168.150.54:2222 WAN (SSH) -> 10.0.0.4:22 VLAN Serveur (SSH)

```

access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 permit 192.168.10.0 0.0.0.31
access-list 10 permit 192.168.11.0 0.0.0.31
access-list 10 permit 192.168.12.0 0.0.0.31
access-list 10 permit 192.168.13.0 0.0.0.31
access-list 10 permit 192.168.14.0 0.0.0.15
access-list 10 permit 172.16.0.0 0.0.0.7
access-list 10 permit 172.16.1.0 0.0.0.127
access-list 10 permit 172.16.2.0 0.0.0.255
access-list 10 permit 10.0.0.0 0.0.0.63

```

Ceci permet d'accéder aux VM et VLAN grâce à une VM "Passerelle", il suffit de se connecter à cette VM puis d'accéder au service souhaité sur l'infrastructure.

Règles de parefeu

```

access-list 10 permit 10.0.0.0 0.0.0.63
access-list 110 permit udp any any eq domain
access-list 110 permit udp any any eq bootps
access-list 110 permit icmp any any
access-list 110 permit tcp any 10.0.0.0 0.0.0.63 eq 389
access-list 110 permit tcp 10.0.0.0 0.0.0.63 any eq 389
access-list 110 permit tcp any 10.0.0.0 0.0.0.63 eq 22
access-list 110 permit tcp 10.0.0.0 0.0.0.63 any eq 22
access-list 110 permit tcp any 10.0.0.0 0.0.0.63 eq 445
access-list 110 permit tcp 10.0.0.0 0.0.0.63 any eq 445
access-list 110 permit tcp any 10.0.0.0 0.0.0.63 eq 139
access-list 110 permit tcp 10.0.0.0 0.0.0.63 any eq 139
access-list 110 permit udp any 10.0.0.0 0.0.0.63 eq netbios-ss
access-list 110 permit udp 10.0.0.0 0.0.0.63 any eq netbios-ss
access-list 110 permit tcp any 172.16.3.0 0.0.0.255 eq 445
access-list 110 permit tcp 172.16.3.0 0.0.0.255 any eq 445
access-list 110 permit tcp any 172.16.3.0 0.0.0.255 eq 139
access-list 110 permit tcp 172.16.3.0 0.0.0.255 any eq 139
access-list 110 permit udp any 172.16.3.0 0.0.0.255 eq netbios-ss
access-list 110 permit udp 172.16.3.0 0.0.0.255 any eq netbios-ss
access-list 110 permit tcp any 10.0.0.0 0.0.0.63 eq 3389
access-list 110 permit tcp 10.0.0.0 0.0.0.63 any eq 3389
access-list 110 permit tcp any 172.16.3.0 0.0.0.255 eq 3389
access-list 110 permit tcp 172.16.3.0 0.0.0.255 any eq 3389
access-list 110 permit tcp any any eq www
access-list 110 permit udp any any eq 80
access-list 110 permit tcp any any eq 443
access-list 110 permit udp any any eq 443
access-list 110 deny ip any any

```

Matrice de flux de Marseille

Source/Destination	WAN	VLAN10, 11, 12, 13, 14	VLAN20	VLAN40	VLAN50
WAN		RIEN	RIEN	RIEN	RIEN
VLAN10, 11, 12, 13, 14	443, 80	TOUT	443, 80	RIEN	53, 67, 389, 445, 3389, 22, 5986

VLAN20	443, 80	RIEN	TOUT	RIEN	RIEN
VLAN40	443, 80	RIEN	443, 80	TOUT	53, 67, 389, 445, 3389, 22, 5986
VLAN50	443, 80	53, 67, 389, 445, 3389, 22, 5986	443, 80	53, 67, 389, 445, 3389, 22, 5986	TOUT

Borne WI-FI

Infos

Système: **OpenWRT**

Adresse IP: **172.16.2.2**

Nom d'utilisateur: **root**

Mot de passe: **Ayp[&uS | Ru(FPK1A**

Accès

<https://wifi.itway.corp>

Les identifiants sont les mêmes en SSH, pour la connexion au réseau Wi-Fi et pour la connexion à l'interface WEB.

ssh root@172.16.2.2

Réseau de Lille

Infos

OS: FreeBSD (PfSense)

Web

URL: <https://192.168.150.65>

Identifiant: admin

Mot de passe: £0:Qf\49&woA

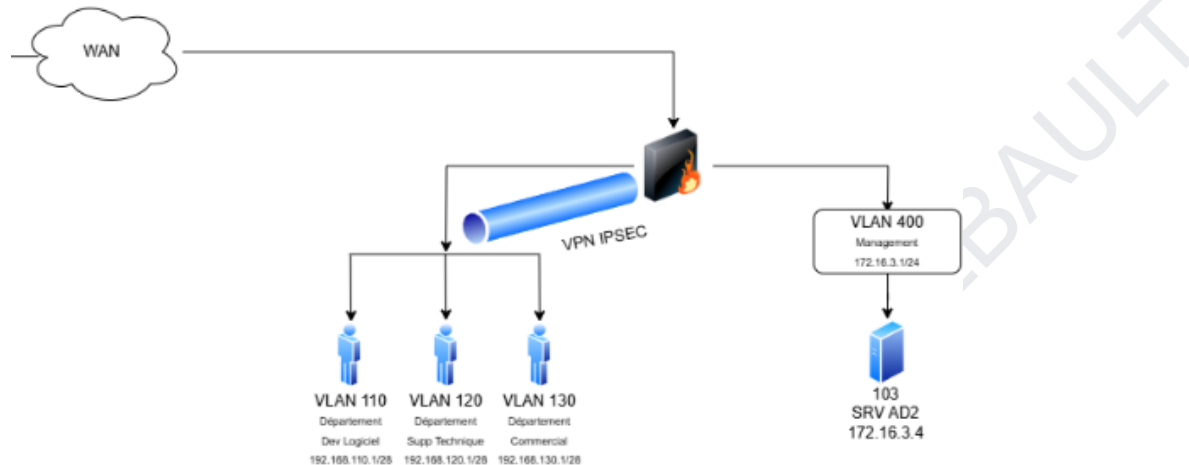


Les 3 PfSense ont les mêmes informations d'identification.

Type: VM

Version: 2.7.2

Schéma



Configuration des VLAN

- VLAN 110 : Département Logiciel → 192.168.110.1/28 (14 IP)
- VLAN 120 : Département Supp Technique → 192.168.120.1/28 (14 IP)
- VLAN 130 : Département Commercial → 192.168.130.1/28 (14 IP)
- VLAN 400 : MANAGEMENT → 172.16.3.1/24 (254 IP)

Configuration du DHCP

VLAN	IP début	IP Fin	DNS	Passerelle	CIDR
110	192.168.110.2	192.168.110.14	10.0.0.3 172.16.3.4	192.168.110.1	192.168.110.1/28
120	192.168.120.2	192.168.120.14	10.0.0.3 172.16.3.4	192.168.120.1	192.168.120.1/28
130	192.168.130.2	192.168.130.14	10.0.0.3 172.16.3.4	192.168.130.1	192.168.130.1/28
400	172.16.3.2	172.16.3.254	10.0.0.3 172.16.3.4	172.16.3.1	172.16.3.1/24

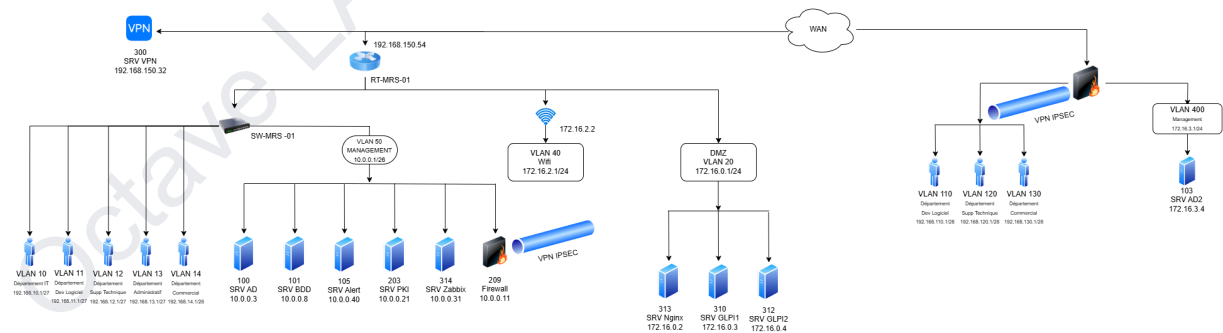
Configuration du NAT

On autorise tous les VLAN à sortir vers le WAN.

Règles de parefeu

Source/Destination	WAN	VLAN110	VLAN120	VLAN130	VLAN400
WAN		RIEN	RIEN	RIEN	RIEN
VLAN110	443, 80	TOUT	RIEN	RIEN	53, 67, 389, 445, 3389, 5986
VLAN120	443, 80	RIEN	TOUT	RIEN	53, 67, 389, 445, 3389, 5986
VLAN130	443, 80	RIEN	RIEN	TOUT	53, 67, 389, 445, 3389, 5986
VLAN400	443, 80	53, 67, 389, 445, 3389, 5986	53, 67, 389, 445, 3389, 5986	53, 67, 389, 445, 3389, 5986	TOUT

Schéma Général



VPN Site à Site

Nous avons monté un VPN IPSEC entre le réseau de Lille et de Marseille.

Ce VPN permet de faire communiquer les VLAN comme suit:

VLAN110, VLAN120, VLAN130 (Utilisateurs Lille) <-> VLAN 50 (Serveurs Marseille)

VLAN 400 (Serveurs Lille) <-> VLAN 10, 11, 12, 13, 14, 20, 40, 50 (Marseille Tous)













































	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/>  Disable	1	tunnel	VLAN110	10.0.0.0/26	ESP	AES (256 bits)	SHA256	Vlan 110	  
<input type="checkbox"/>  Disable	2	tunnel	VLAN120	10.0.0.0/26	ESP	AES (256 bits)	SHA256	Vlan 120	  
<input type="checkbox"/>  Disable	3	tunnel	VLAN130	10.0.0.0/26	ESP	AES (256 bits)	SHA256	Vlan 130	  
<input type="checkbox"/>  Disable	4	tunnel	VLAN400SERVEURS	10.0.0.0/26	ESP	AES (256 bits)	SHA256	Vlan 400	  
<input type="checkbox"/>  Disable	5	tunnel	VLAN400SERVEURS	192.168.10.0/24	ESP	AES (256 bits)	SHA256	Vlan 400	  
<input type="checkbox"/>  Disable	6	tunnel	VLAN400SERVEURS	192.168.11.0/24	ESP	AES (256 bits)	SHA256	Vlan 400	  
<input type="checkbox"/>  Disable	7	tunnel	VLAN400SERVEURS	192.168.12.0/24	ESP	AES (256 bits)	SHA256	Vlan 400	  
<input type="checkbox"/>  Disable	8	tunnel	VLAN400SERVEURS	192.168.13.0/24	ESP	AES (256 bits)	SHA256	Vlan 400	  
<input type="checkbox"/>  Disable	9	tunnel	VLAN400SERVEURS	192.168.14.0/24	ESP	AES (256 bits)	SHA256	Vlan 400	  
<input type="checkbox"/>  Disable	10	tunnel	VLAN400SERVEURS	172.16.0.0/24	ESP	AES (256 bits)	SHA256	Vlan 400	  
<input type="checkbox"/>  Disable	11	tunnel	VLAN400SERVEURS	172.16.2.0/24	ESP	AES (256 bits)	SHA256	Vlan 400	  

Tableau de synthèse des VMs et Conteneurs

Le nom des VM et des conteneurs suit la forme SystèmeServiceNuméroSite

La connexion SSH aux systèmes linux ne peut pas être faite avec l'utilisateur root, il y a donc à chaque fois un utilisateur **ssh**.

Il faut ensuite s'élever avec la commande : **su -**

Pour se connecter à l'infrastructure il faut passer par une VM passerelle la VM 111. Soit en RDP (MSTSC) soit en SSH sur le port 2222:

ssh test@192.168.150.54 -p 2222

ID PVE	Nom PVE	Utilisateur	Mot de passe	VLAN	IP
x	Proxmox	root ssh	DR.5Gn"%mA'+B@v z"I3S386xY>B	x	http://192.168.150.22:8006
100	WinServ1MarsAD	Administrateur	GcblHDzd12516!	50	10.0.0.3
103	WinServ2LilleAD	Administrateur	GcblHDzd12516!	400	172.16.3.4
101	DebSGBD1Mars	root ssh	-QVHw]sL)mdHcq@n 2i-4cN\$K(4{3	50	10.0.0.8
105	DebAlert1Mars	root	OpMLkjH522*	50	10.0.0.40
111	Passerelle-Mrs	test	admin		192.168.150.

		octave-deleg	Annogamer84!		54 Port ssh: 2222
203	DebPki1Mars	root service ansible	ApatMf598* PadniTh412* annogamer	50	10.0.0.21
208	DebPfSenseLil	root	£0:Qf\49&woA	X	192.168.150. 65
209	DebPfSenseMars	root	£0:Qf\49&woA	50	10.0.0.11
210	RT-MRS-02 (Redondance du RT Cisco: éteint)	root	£0:Qf\49&woA	X	192.168.150. 54
300	DebServVPN	root ssh	Zsxxwqa123456! Aqwxsz123456!	X	192.168.150. 32
311	DebGLPI1Mars	root ssh	AzedGh239* AzedGh239*	20	172.16.0.3
312	DebGLPI2Mars	root ssh	AzedGh239* AzedGh239*	20	172.16.0.4
400	UbuWazuh1Mars	octave	AzedGh239*	50	10.0.0.27
313	DebNginx1Mars	root ssh ansible	AzedGh239* AzedGh239* annogamer	20	172.16.0.2
314	DebZabbix1Mars	root service ansible	OpMLkjH522* FrTuBn533* annogamer	50	10.0.0.31
104	DebSquid1Mars	root ssh	AzedGh239* annogamer	50	10.0.0.23
106	DebAnsible1Mars	root ssh	annogamer annogamer	50	10.0.0.24

Fail2Ban étant installé sur toutes les VM, veillez à ne pas vous tromper lors de la saisie, vous n'avez que trois essais.

WinServ1MarsAD: Service d'authentification

Infos

OS: Windows Serveur 2019

Type: VM

Nom de la machine WinServ1MarsAD -> **SRV-ADDS-01**

Nom de la machine WinServ2MarsAD -> **SRV-ADDS-02**

Ces deux AD sont en réplication.

Utilisateurs et Groupes:

Utilisateur	Mot de passe	UO	Groupe
it_MARS	Ojnht759*	Marseille>dep_it	Dep_IT
devlog_mars	Ogjue548*	Marseille>dep_devlogiciel	Dep_DevLogiciel
supptech_mars	Ohfyf236*	Marseille>dep_supptech	Dep_SuppTech
administratif_MARS	Okhfe965*	Marseille>dep_administratif	Dep_Administratif
comm_mars	Onbhf145*	Marseille>dep_comm	Dep_Comm
devlog_lille	Ojehf896*	Lille>dep_devlog	Dep_DevLogiciel
supptech_lille	Oeyfb635*	Lille>dep_supptech	Dep_SuppTech
comm_lille	Opkg459*	Lille>dep_comm	Dep_Comm
ansible	IY(*xeal8y{m{LHW	Admin>User	admin_local

Partages SMB

Administratif	C:\partage\Administratif	SMB	Non-cluster
certs	C:\Partage\certs	SMB	Non-cluster
Commercial	C:\partage\Commercial	SMB	Non-cluster
dev	C:\partage\dev	SMB	Non-cluster
fond	C:\Partage\fond	SMB	Non-cluster
logiciels	C:\partage\logiciels	SMB	Non-cluster
NETLOGON	C:\Windows\SYSVOL\sysvol\itway....	SMB	Non-cluster
Support-IT	C:\partage\it	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster

Le dossier **certs** contient la **CA** de la **PKI**.

Le dossier **fond** contient les fonds d'écran.

Le dossier **logiciels** contient les logiciels installés sur les postes.

Le dossier **Scripts** contient les scripts d'activation de **winrm** pour Ansible.

Les autres dossiers sont des dossiers partagés pour les groupes utilisateurs et sont déployés par GPO.

Enregistrement DNS



FQDN	IP
glpi.itway.corp	172.16.0.2 (NGINX)
alert.itway.corp	172.16.0.2 (NGINX)
db.itway.corp	10.0.0.8
wazuh.itway.corp	10.0.0.27
zabbix.itway.corp	172.16.0.2 (NGINX)
srv-adds-01	10.0.0.3
srv-adds-02	172.16.3.4

GPO

Nom	Action
applications	Installer wireshark sur tous les postes
bg	Mets un fond d'écran sur tous les postes
Certs	Ajoute l'autorité de certification sur les postes
Remove welcome msg	Enlève le message de bienvenue à la première ouverture de edge.
Prtg-it, prtg-admini, prtg-comm, prtg-devlog	Ajouter le mappage de partage (P:) sur les utilisateurs en fonction du groupe.
forcePorxy	Force l'utilisation du proxy pour les clients
winrm	Script powershell qui active winrm pour Ansible

Serveur Radius & AD CS

Le service NPAS est installé ainsi que le service AD CS. Le service AD CS a permis la génération d'un certificat pour la borne wi-fi et le service NPAS permet d'utiliser la borne Wi-Fi en client RADIUS.

Clients RADIUS			
 Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau.			
Nom convivial	Adresse IP	Fabricant du périphérique	État
 AP-G10	172.16.2.2	RADIUS Standard	Activé

DebSGBD1Mars: Base de donnée MySQL (avec PhpMyAdmin)

Infos

OS: Debian 12

Type: Conteneur

Accès Web

URL: <https://db.itway.corp/phpMyAdmin>

Utilisateur : root

MDP : -QVHw]sL)mdHcq@n

Présentation

```
mysql> show databases;
+-----+
| Database |
+-----+
| glpi_db   |
| information_schema |
| mysql     |
| performance_schema |
| sys       |
+-----+
5 rows in set (0.03 sec)
```

Solution de sauvegarde

Fréquence

Des sauvegardes ont été mises en place directement dans Proxmox.

Les snapshots se font sur toutes les VM en simultanément tous les dimanches à 1h00.

Node:	pve-samy	Notification mode:	Default (Auto)
Storage:	VM-BACKUP	Send email to:	
Schedule:	sun 01:00	Send email:	Always
Selection mode:	Include selected VMs	Compression:	ZSTD (fast and good)
		Mode:	Snapshot
		Enable:	<input checked="" type="checkbox"/>

Gestion

Il y a un roulement au niveau des backup afin d'éviter de saturer l'espace disponible. Proxmox ne garde que les cinq dernières sauvegardes.

General	Retention	Note Template	Advanced
<input type="checkbox"/> Keep all backups			
Keep Last:	5	Keep Hourly:	
Keep Daily:		Keep Weekly:	
Keep Monthly:		Keep Yearly:	

DebGLPI1Mars: Gestion des incidents avec GLPI

Infos

OS: Debian 12

Type: Conteneur

Accès Web

URL: <https://glpi.itway.corp/>

Utilisateur : glpi

MDP : admin

Source de connexion: Base de donnée GLPI

Il y a deux GLPI en redondance grâce à NGINX (DebGLPI2Mars).

Présentation de l'interface d'administration

- Tableau de bord.
- Menus principaux (Gestion, Assistance, Administration....).

Création d'un ticket de support

- Démontrer comment créer un ticket de support.
- Assigner le ticket à un technicien.

Gestion d'un élément du parc informatique

- Ajouter un nouvel ordinateur au parc.
- Démontrer la gestion des inventaires (logiciels, matériels, etc.).

DebPki1Mars: La PKI

Infos

OS: Debian 12

Type: VM

Autorité de certification

Le fichier **ca.crt** est notre autorité de certification.

Mot de passe de la CA: **Bonjourlaphrase**

Fichiers

Dossier des nouveaux certificats: **/etc/pki/newcerts**

Dossier des clés: **/etc/pki/private**

Utilisation

Il faut déplacer les certificats (**.crt** et **.key**) dans **/home/service** puis se connecter en **sftp** à la PKI avec: **sftp service@10.0.0.21** pour pouvoir les récupérer sur la machine qui en à besoin.

Supervision

DebZabbixMars: Services

Pour la supervision des services, nous avons choisi d'utiliser Zabbix.

Accès Web

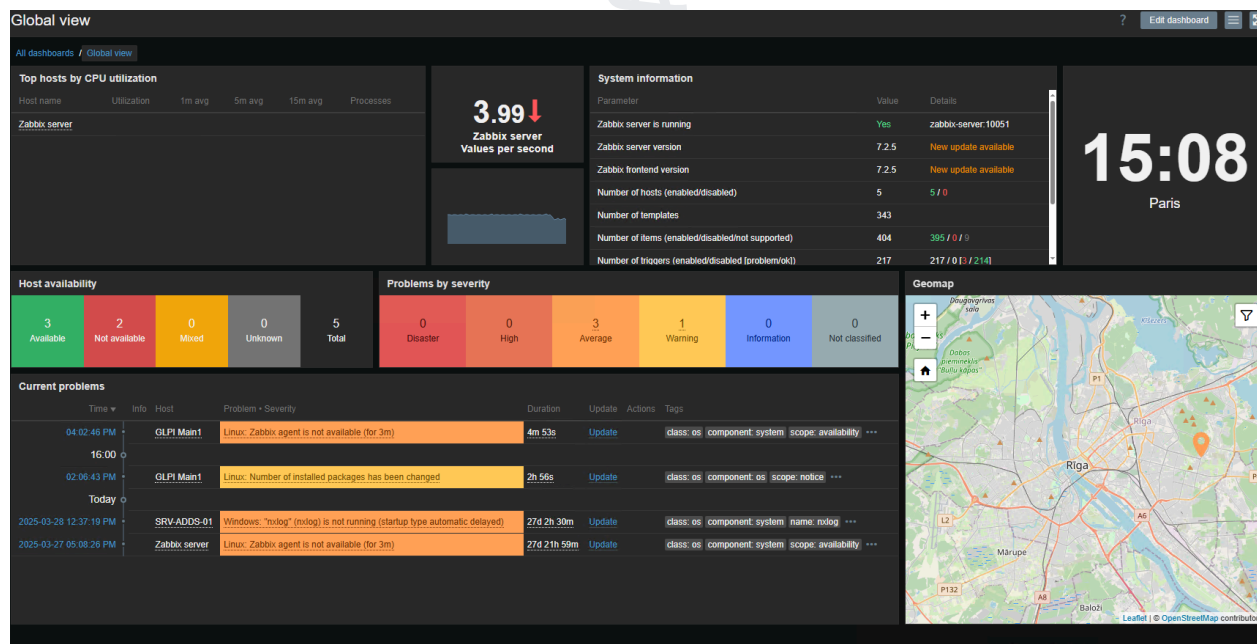
URL: <https://zabbix.itway.corp>

Identifiant: **Admin**

Mot de passe: **zabbix**

Présentation

Le panneau de présentation en "global view" est assez simple. Il montre le nombre d'hôtes opérationnels, les problèmes par ordre de gravité, les problèmes en cours, et quelques autres informations de base comme l'état du serveur zabbix lui-même.

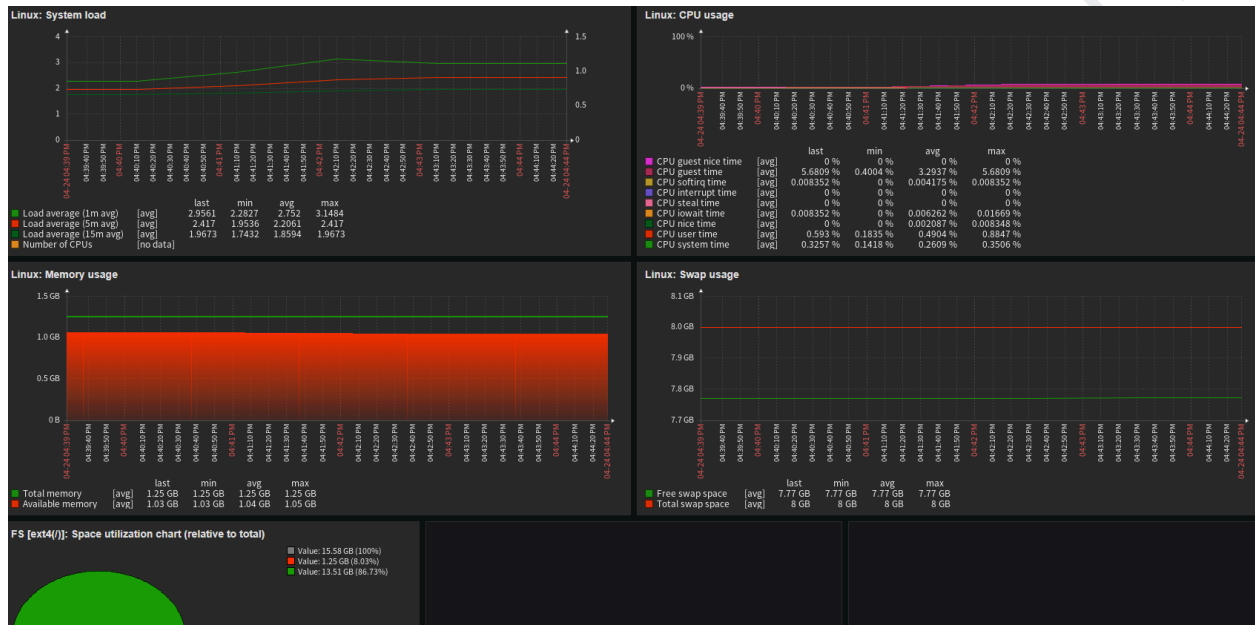


Nous avons accès aux logs et aux états de santé de chacune des machines sur lequel il y a un agent zabbix.

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
GLPI Main1	172.16.0.3:10050	26%	class: os target: linux	Enabled	Latest data 59	1	Graphs 11	Dashboards 3	Web
GLPI Redo1	172.16.0.4:10050	26%	class: os target: linux	Enabled	Latest data 59	Problems	Graphs 11	Dashboards 3	Web
SRV-ADDS-01	10.0.0.3:10050	26%	class: os target: windows	Enabled	Latest data 111	1	Graphs 12	Dashboards 3	Web
SRV Base de donnée	10.0.0.8:10050	26%	class: os target: linux	Enabled	Latest data 59	Problems	Graphs 11	Dashboards 3	Web
Zabbix server	127.0.0.1:10050	26%	class: os class: software target: linux	Enabled	Latest data 116	1	Graphs 5	Dashboards 4	Web

Displaying 5 of 5 found

Parmi toutes les informations à notre disposition, nous pouvons avoir des **dashboard** avec l'usage du disque, ou encore des alertes qui remontent aux administrateurs en fonction du niveau de l'alerte.



Action

Name: Report problems to Zabbix administrators

Type of calculation: And/Or (A or B or C or D or E or F or G or H)

Label	Name	Action
A	Trigger equals GLPI Redo1: Linux: FS [/]: Filesystem has become read-only	Remove
B	Trigger equals GLPI Redo1: Linux: FS [/]: Running out of free inodes	Remove
C	Trigger equals GLPI Redo1: Linux: FS [/]: Running out of free inodes	Remove
D	Trigger equals GLPI Redo1: Linux: FS [/]: Space is critically low	Remove
E	Trigger equals GLPI Redo1: Linux: FS [/]: Space is low	Remove
F	Trigger equals GLPI Redo1: Linux: Getting closer to process limit	Remove
G	Trigger equals GLPI Redo1: Linux: GLPI Redo1 has been restarted	Remove
H	Trigger equals GLPI Redo1: Linux: High CPU utilization	Remove

Enabled: ☐

*** At least one operation must exist.**

Buttons: Update, Clone, Delete, Cancel

DebAlert1Mars: Réseau

Pour la supervision réseau nous utilisons **PiAlert** car le projet **Eyes of Network** à été arrêté.

Infos

OS: Debian 12

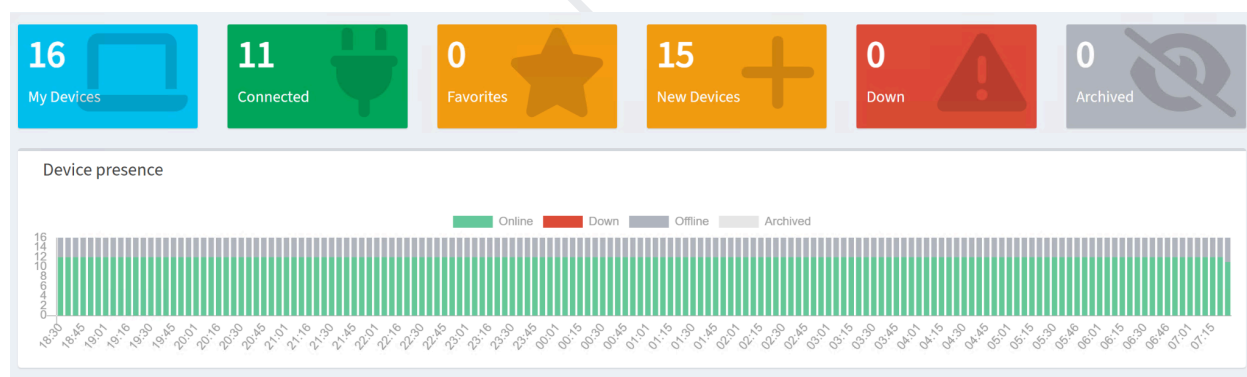
Type: VM

Accès Web

URL: <https://alert.itway.corp/>

Présentation

Le dashboard est simple et efficace il permet de visualiser l'ensemble des appareils connectés au réseau et de mettre un TAG sur les nouveaux, de sorte à alerter le technicien qu'un appareil vient de se connecter. Afin qu'il puisse vérifier la légitimité.



DebNginx1Mars: Equilibrage des charges

Infos

OS: Debian 12

Type: Conteneur

Présentation

Pour l'équilibrage des charges nous utilisons NGINX, ce service nous permet également de faire du **Reverse Proxy** et du **Failover**. La redondance du serveur GLPI par exemple.

Exemple de configuration (GLPI)

Fichier de configuration: /etc/nginx/nginx.conf

```
upstream glpi {  
    server 172.16.0.3 weight=5 max_fails=3;  
    server 172.16.0.4 weight=1 max_fails=3;  
}
```

La configuration est simple tous les trois clients une redirection est faite vers l'autre serveur.

UbuWazuh1Mars:

Infos

OS: Ubuntu server 22

Type: VM

Accès Web

<https://wazuh.itway.corp>

Utilisateur: admin

Mot de passe: DbS02ZyROjdL?9cQ6uvjJtwgCt8MrI9u

Configuration

Logs remontée grâce à Wazuh

Log

Nous avons choisi de remonter les informations suivantes:

- Modification majeure de l'AD
- Connexions SSH
- Faille de sécurité
- Mise à jour nécessaire

Utilisation

L'utilisation est simple, il faut se connecter à l'interface WEB et dans un premier temps s'assurer qu'aucune alertes aient un niveau supérieur à "Medium Severity"

DebSquid1Mars: Serveur Proxy

Infos

OS: Debian 12

Type: Conteneur

Configuration

Le fichier de configuration se trouve à l'emplacement suivant:

/etc/squid/squid.conf

Les réseaux autorisé

Marseille

10.0.0.0/26 -> VLAN Serveur Marseille

192.168.10.0/27 -> VLAN Utilisateur Marseille

192.168.11.0/27 -> VLAN Utilisateurs Marseille

192.168.12.0/27 -> VLAN Utilisateurs Marseille

192.168.13.0/27 -> VLAN Utilisateurs Marseille

192.168.14.0/27 -> VLAN Utilisateurs Marseille

172.16.2.1/24 -> VLAN Wi-Fi Marseille

Lille

192.168.110.0/28 -> VLAN Utilisateurs Lille

192.168.120.0/28 -> VLAN Utilisateurs Lille

192.168.130.0/28 -> VLAN Utilisateurs Lille

172.16.3.1/24 -> VLAN Serveur Lille

Les ports autorisé

- HTTP (80)
- HTTPS (443)
- FTP (21)

Les domaines bloqués sont:

- youtube.com
- youtube.fr
- instagram.com

Exemple

Voici un exemple de configuration :

```
##### ACL #####

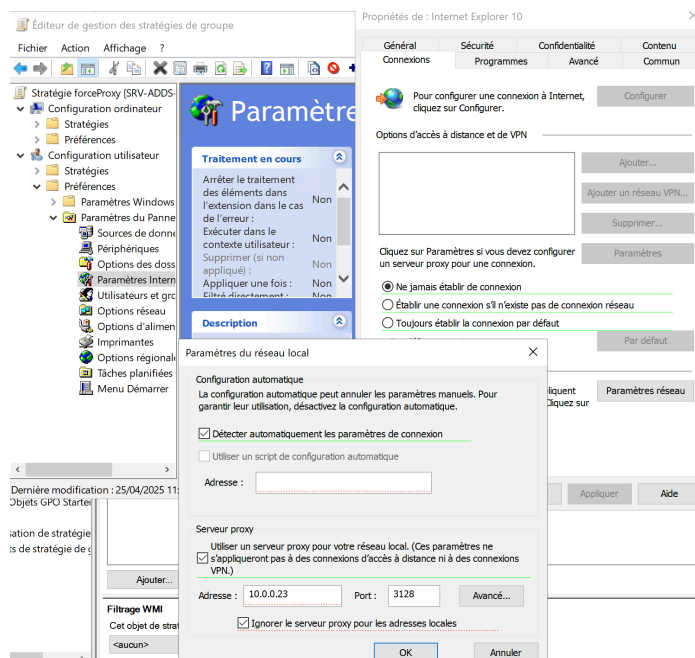
acl all src all
acl lan src 10.0.0.1/26
acl lan src 192.168.10.0/27
acl lan src 192.168.11.0/27
acl lan src 192.168.12.0/27
acl lan src 192.168.13.0/27
acl lan src 192.168.14.0/27
acl lan src 172.16.2.1/24
acl lan src 192.168.110.0/28
acl lan src 192.168.120.0/28
acl lan src 192.168.130.0/28
acl lan src 172.16.3.1/24

acl Safe_ports port 80 # Port HTTP = Port 'sure'
acl Safe_ports port 443 # Port HTTPS = Port 'sure'
acl Safe_ports port 21

acl deny_domain url_regex -i "/etc/squid/denydomain.txt"
```

GPO

On a forcé l'utilisation du proxy par GPO.



DebAnsible1Mars: Serveur Ansible

Infos

OS: Debian 12

Type: Conteneur

Configuration

La configuration de Ansible se fait comme suit:

Il faut d'abord publier la clé publique SSH du serveur sur les futurs clients qui ont un utilisateur avec les droits sudo (ici l'utilisateur est ansible) pour que le serveur se connecte sans mot de passe. Ensuite il faut écrire un playbook qui comporte les étapes à suivre comme montré ci-dessous

```

- name: Installer Wireshark sur les machines Linux
  hosts: linux
  become: true # sudo
  become_method: sudo
  tasks:
    - name: Mettre a jour APT
      apt:
        update_cache: yes
    - name: Installer Wireshark
      apt:
        name: wireshark
        state: present

```

Hôtes

Les hôtes que nous avons configurés sont les suivants:

- DebPki1Mars
- DebNginx1Mars
- DebZabbix1Mars

Déploiements

Nous avons déployé **Wireshark** après une mise à jour (apt update) sur les hôtes Linux.

Pas besoin de le faire sur Windows, nous l'avons fait par GPO.

Exemple

```
ansible-playbook /etc/ansible/depl-wireshark/wireshark-linux.yml
```

```

root@DebAnsible1Mars:/etc/ansible# ansible-playbook /etc/ansible/depl-wireshark/wireshark-linux.yml

PLAY [Installer Wireshark sur les machines Linux] *****

TASK [Gathering Facts] *****
ok: [DebNginx1Mars]
ok: [DebPki1Mars]
ok: [DebZabbix1Mars]

TASK [Mettre a jour APT] *****
ok: [DebNginx1Mars]
ok: [DebPki1Mars]
changed: [DebZabbix1Mars]

TASK [Installer Wireshark] *****
ok: [DebNginx1Mars]
ok: [DebPki1Mars]
changed: [DebZabbix1Mars]

PLAY RECAP *****
DebNginx1Mars      : ok=3    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
DebPki1Mars        : ok=3    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
DebZabbix1Mars     : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

```

Annexe 10

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

SESSION 2025

ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification ¹		SISR
-----------------------------	--	-------------

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un service d'authentification	Serveur AD Windows Server 2019 Nom de la machine : WinServ1MarsAD Nom d'utilisateur : Administrateur Mot de Passe : GcblHDzd12516! Adresse IP : 10.0.0.3	
Un SGBD	Debian Nom de la machine : DebSGBD1Mars Nom d'utilisateur : ssh Mot de Passe : 2i-4cN\$K(4{3 Nom d'utilisateur root : root Mot de passe root : -QVHw]sL)mdHcq@n Adresse IP : 10.0.0.63	

¹ Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

Un accès sécurisé à internet	Oui, sur tous les postes.	
Un environnement de travail collaboratif	Discord, Office 365	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (<i>open source</i>)	WinServ1MarsAD (Windows serveur 2019), DebSGBD1Mars(Debian)	

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Snapshots du proxmox effectuée tous les dimanches à minuit.	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Partage active directory Serveur AD Windows Server 2019 Nom de la machine : WinServ1MarsAD Nom d'utilisateur : Administrateur Mot de Passe : GcblHDzd12516! Adresse IP : 10.0.0.3	
Deux types de terminaux dont un mobile (type <i>smartphone</i> ou encore tablette)	Téléphone connecté en WI-Fi et ordinateur portable en Ethernet	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	GLPI Debian Nom de la machine : DebGLPI1Mars Nom d'utilisateur : root Mot de Passe : AzedGh239* Adresse IP : 172.16.0.3	
Détection et prévention des intrusions	Fail2Ban est installé et l'utilisateur root est désactivé en SSH. Zabbix Debian Nom de la machine : DebZabbixMars Nom d'utilisateur : root	

	Mot de Passe : OpMLkjH522* Adresse IP : 10.0.0.63	
Chiffrement	PKI avec OpenSSL Debian Nom de la machine : DebPki1Mars Nom d'utilisateur : service Mot de passe : PadniTh412* Nom d'utilisateur root : root Mot de passe root : ApatMf598* Adresse IP : 10.0.0.63	
Analyse de trafic	Wireshark est installé sur tous les postes.	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Parefeu et règles ACL Cisco et segmentation en VLAN.	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Zabbix Debian 12 Nom de la machine : DebZabbix1Mars Nom d'utilisateur : root Mot de Passe : OpMLkJH522* Adresse IP : 10.0.0.63	
Un logiciel d'analyse de trames	Wireshark est installé sur tous les postes.	
Un logiciel de gestion des configurations	Ansible Debian 12 Nom de la machine : DebAnsible1Mars Nom d'utilisateur : ssh Mot de Passe : annogamer Nom d'utilisateur root : root Mot de Passe root : annogamer Adresse IP : 10.0.0.24	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Nous avons un VM qui sert de passerelle pour accéder à l'infra et ses différentes VLANs et VM. Deux accès sont possibles. En SSH : ssh test@192.168.150.54 -p 2222	

	<p>Nom d'utilisateur : test Mot de passe : admin</p> <p>En RDP : 192.168.150.54 (Redirection NAT à travers le routeur) Nom d'utilisateur : test Mot de passe : admin</p>	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	<p>PiAlert Debian Nom de la machine : DebAlert1Mars Nom d'utilisateur : root Mot de Passe : OpMLkJH522* Adresse IP : 10.0.0.40</p>	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	<p>Mise en place d'une DMZ sécurisée avec règles de parefeu stricte. Serveur Proxy</p> <p>Debian Nom de la machine : DebSquid1Mars Nom d'utilisateur : ssh Mot de Passe : annogamer</p> <p>Nom d'utilisateur root : root Mot de passe root : AzedGh239* Adresse IP : 10.0.0.23</p>	
Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	<p>AD redondant : WinServ1MarsAD WinServ2MarsAD</p>	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	<p>AD redondant : WinServ1MarsAD WinServ2MarsAD</p> <p>Un serveur NGINX avec deux serveurs Web GLPI en redondance. Debian Nom de la machine : DebNginx1Mars</p>	

	Nom d'utilisateur : ssh Mot de Passe : annogamer Nom d'utilisateur root : root Mot de passe root : AzedGh239* Adresse IP : 172.16.0.2	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	NGINX Debian Nom de la machine : DebNginx1Mars Nom d'utilisateur : ssh Mot de Passe : annogamer Nom d'utilisateur root : root Mot de passe root : AzedGh239* Adresse IP : 172.16.0.2	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	Un VPN site à site entre Marseille et Lille	
Une solution permettant le déploiement des solutions techniques d'accès		
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de <i>scripting</i>		
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau		