

BTS SIO DOCUMENTATION TECHNIQUE FICHE n°1

Épreuve E6



Alexandre BONGRAND 07/05/2025



Documentation technique fiche nº1

Suivi des modifications

Version	Référence	Auteur	Date	Commentaires
Α	Documentation technique fiche nº1	Alexandre	25/04/2025	Création

.....

Objet :

Documentation technique fiche nº1 - Projet E6

Diffusion :

BTS SIO – Étudiants BTS SIO.

Développement :

Table des matières

WINDOWS SERVEUR Installation AD DS & DNS	
Mise en place des GPOs	5
Partage de fichiers	7
PFSENSE	9
Mise en place des règles de Pare-feu	9
VLAN 10	9
VLAN 20	
VLAN 30	
SERVEUR DEBIAN	
Installation Docker et Portainer	
Portainer	12
Wazuh	13
Zabbix	15
Installation Base de données	17



WINDOWS SERVEUR

Dans un premier temps, j'ai installé Windows Server 2022 afin de mettre en place un contrôleur de domaine (AD DS), un serveur DNS, ainsi qu'un partage de fichiers.

Ces services permettront aux utilisateurs de l'entreprise BONGRAND de travailler de manière collaborative.

L'installation de Windows Server 2022 s'effectue de la même manière que celle d'un poste client sous Windows 10.

🖆 Configuration du système d'exploitation Microsoft Server	🕞 💰 Configuration du système d'exploitation Microsoft Server
	Sélectionner le système d'exploitation à installer
Microsoft	Système d'exploitation Architecture Date de modi
	Windows Server 2022 Standard (expérience de bureau) x64 07/08/2021
	Windows Server 2022 Datacenter x64 07/08/2021
	Windows Server 2022 Datacenter (expérience de bureau) x64 07/08/2021
Langue à installer : <mark>Français (France) ▼</mark>	
Eormat horaire et monétaire : Français (France)	Description : (Recommandé) Cette option ignore la majeure partie de l'environnement graphique Windows. À gérer avec une invite de commandes et PowerShell, ou à distance avec Windows Admin Center ou
<u>C</u> lavier ou méthode d'entrée : Français	d'autres outils.
Entrez la langue et les préférences de votre choix et cliquez sur Suivant pour continuer.	Suivant
🚱 🔬 Microsoft Server Operating System Setup	Microsoft Server Operating System Setup
Where do you want to install the operating system?	Installing Microsoft Server Operating System
Name Total size Free space Type	Status
Drive 0 Unallocated Space 80.0 GB 80.0 GB	Copying Microsoft Server Operating System files Getting files ready for installation (59%) Installing features Installing updates Finishing up
%p Befresh X Delete ✓ Eormat ★ Ngw ♦ Load driver ♣ Egtend	
Next	

Une fois le système installé, nous pouvons procéder à l'installation des services nécessaires pour répondre aux besoins de l'entreprise BONGRAND.

Installation AD DS & DNS

Pour installer l'Active Directory, nous allons dans fonctionnalité de notre serveur et ajout d'une fonctionnalité.

Pour installer un AD, certain prérequis sont obligatoire, comme une adresse IP statique et installer le service DNS (Domaine Name Service).

Projet E6 Version : A Documentation technique fiche nº1 Date : 25/04/2025 × 2 🖬 0 estDnsZo Hôte (A) Hôte (A) Hôte (A) 192.168.10.250 23/04/2025 23:00:00 192.168.50.250 2 168 50 25 ias (CN Hôte (A)

En installant l'AD, nous créerons un domaine (une nouvelle forêt), notre domaine s'appellera bongrand.local

🔶 🗾 🥥

0 🚍 🧎 🛹 📕

P Tapez ici pour effectuer une recherche

Une fois notre domaine créé, nous pouvons ajouter nos utilisateurs. Pour ajouter les utilisateurs à l'Active Directory, j'ai d'abord fait un excel avec tous les utilisateurs de l'organigramme.

J'ai enregistré cet Excel en « .csv (point-virgule) », ce qui va nous permettre de faire un script d'ajout d'utilisateur.

Grâce à mon fichier.csv, j'ai pu créer un script powershell, qui va ajouter chaque utilisateur dans l'AD dans un groupe que j'ai nommé « Utilisateurs ».

Projet E6

.....



Documentation technique fiche n°1

Date : 25/04/2025

<pre># Chemin vers le fichier CSV contenant les inf \$cheminCSV = "C:\Users\Administrateur\Desktop\</pre>	formations des utilisateurs \user.csv"	
<pre># Lire les utilisateurs à partir du fichier CS \$utilisateurs = Import-Csv -Path \$cheminCSV</pre>	5V	
∃foreach (Sutilisateur in Sutilisateurs) { # Construire le nom d'utilisateur (login) SnomUtilisateur = (Sutilisateur.Prenom + '	au format "prenom.p" "." + <mark>\$utilisateur</mark> .Nom.Substring(0,1)).ToLower()	
<pre># Construction du nom complet \$nomComplet = \$utilisateur.Prenom + " " +</pre>	\$utilisateur.Nom	
<pre># Définir l'OU (Unité d'Organisation) cibl \$ou = "OU=Utilisateurs,DC=lanlrt,DC=monEpi</pre>	le où les utilisateurs seront créés icerie,DC=eu"	
<pre># Chemin d'accès à l'AD \$cheminAD = "CN=" + \$nomComplet + "," + \$nomComplet + \$nomComplet + "," + \$no</pre>	bu	
<pre># Définir un mot de passe par défaut (peut \$motDePasse = ConvertTo-SecureString "Kiri</pre>	t être modifié selon vos besoins) ikou202409!" -AsPlainText -Force	
<pre># Créer l'utilisateur dans Active Director New-ADUser -SamAccountName SnomUtilisateur -UserPrincipalName SnomUtilisateur -Name SnomComplet -DisplayName SnomComplet -GivenName Sutilisateur.Prenom -Surname Sutilisateur.Nom -Path Sou -AccountPassword SmotDePasse -Enabled Strue -PasswordNeverExpires Strue * Le mot</pre>	y t de passe n'expire jamais	
Utilisateurs et ordinateurs Active	Nom	Туре
Requêtes enregistrées	🛃 alexandre bongrand	Utilisateur
✓ jii bongrand.local	🛃 Jean Bon	Utilisateur
V BONGRAND	💄 nextcloud	Utilisateur
Groupes		
Urdinateurs		

Une fois les utilisateurs crées, j'ai crée un dossier personnel pour chaque utilisateurs.



Pour les ordinateurs, lorsque l'on va ajouter un ordinateur à notre domaine, il va automatiquement s'ajouter à computers, je les déplace dans le groupe "Ordinateurs" que j'ai créé afin de pouvoir lier des GPOs à ce groupe.

Groupes pour les droits :

Projet E6



Date: 25/04/2025

Utilisateurs et ordinateurs Active Directory									
Fichier Action Affichage ?									
🗢 🔿 🙋 📊 📋 🖾 🤅	🛛 🖬 🐍 📚 🛅 🍸 💆 🍇								
 Utilisateurs et ordinateurs Active Requêtes enregistrées Bongrand.local BONGRAND Groupes Utilisateurs Ordinateurs Builtin Computers Domain Controllers ForeignSecurityPrincipal: 	Nom Admin-local BONG-GS-Admin-M BONG-GS-Comptable-M BONG-GS-Direction-M BONG-GS-partage-M BONG-GS-Partageinfo\$-M BONG-GS-Partinf\$Setup-L BONG-GS-RH-L BONG-GS-RH-L BONG-GS-RH-M	Type Groupe de sécurité - Global Groupe de sécurité - Global							
Managed Service Accour									

Mise en place des GPOs

J'ai créé des GPO afin de rendre l'utilisateur "Alexandre Bongrand" administrateur des postes qu'il utilise. Cela a pour but de lui permettre d'effectuer des manipulations d'administration sur les postes (installation de logiciels, paramétrage de Windows, etc.).

GPO admin local :

Gestion de stratégie de groupe						– a ×				
📓 Fichier Action Affichage Fenêtre ?						- 8 ×				
← ➡ 🙇 📰 🙆 🖬										
Gestion de stratégie de groupe Cartet : bongrand.local Songrand.local Defaul: Domaine Olicy Songrand.local Defaul: Domain Olicy SoNGRAND SONGRAND Groupes	Admin Syst Ennolve Delaits Paraméters Délégation Lieisons Afficher is saisons à cet emplacement : bengrand local Les sites, domaines et unités d'organisation suivants sont lés à cet objet GPO : Emplacement Apolou Lien activé Chemin d'acobs									
Admin Syst	Ordinateurs	Non	Oui	bongrand.local/BONGRAND/Ordinateurs						
Chjets GPO Starter	2 Utilisations	Non	Oui	bongrand local/BONGRAND/Utilisateurs						
 Modélisation de stratégie de groupe 	Ellerer de sécurité									
Résultats de stratégie de groupe	Filtrage de securite	ent aux groupe	es utilisateurs et o	rinateurs suivants :						
	Nom R, Admin-local (BONGRAND/Admin-local) Utilizateurs authentifiés									
	Ajouter Supprimer	Propriétés	5							
	Filtrage WMI Cet objet de stratégie de groupe est lié au filtre WM <aucun></aucun>	suivant : ~	Ouvrir		Activer Windows Accédez aux paramètres	: pour activer Windows.				
	herche 🗏 💽 👝	. 🧇		ž <u>I 4</u> 🖻		\ ☐ 4 <mark>8 28/04/2025</mark> ☐				

			Pro	ojet E6		Versio	n : A
E DE FORMATION			Documentation	technique fiche n°	1	Date : 25/0	04/2
Gestion de stratégie de g	groupe hage Fenêtre ?					- 0	× - 8 ×
Gestion de stratégie de g	groupe	Admin_Sy	vst Détaile Paramètres Défénsion				
 Maines Maines	al romain Policy		Groupes restreints				^
- BONGRAM	ND		Grouper	Membres	Membre de		
 ✓ Group ✓ Group 	ateurs		Admin_local	BONGRAND\ Admin-local	BUILTIN\Administrateurs		
Ad	Jmin_Syst	Préf	érences				
Vilisa	dmin_Syst	Pa	ramètres du Panneau de configuration				
> 📓 Domain C	ontrollers						
 Version of the second se	stratégie de groupe Syst		Julisateurs et groupes locaux				
I Defau	It Domain Controllers Policy		Groupe (nom : Administrateurs)				
🧾 Defaul	It Domain Policy		Administrateurs (ordre : 1)				
> 🧊 Objets GP	O Starter		Groupe local				
 Sites Modélication do la 	stratégie de groupe		Action	Mettre à	jour		
Résultats de strat	tégie de groupe		Propriétés				
			Nom du groupe	Adminis	strateurs		
			Supprimer tous les utilisateurs membres Supprimer tous les groupes de membres	Active			
		111	Acoutes des membres				
			Ajouter des membres Administrateur				111
			Ajouter des membres Administrateur BONGRANDI Admin-local	\$-15-2	1-568891775-1310009993-2218769375-1104		
			Ajouter des membres Administrateur BONGRANDI Admin-local Commun	\$1-52	1.568891775-1310009993-2218769375-1104		
			Ajouter das membres Administratur BONGRANDI Adminiocal Commun Options	5152	1-568891775-1310009993-2218769375-1104		
			Ajottet des mentions Administratur BONGRANDI Admin-local Commun Options Intercorps le tratement des éléments sur cette extension Descenter auf Aleman Union (2 d'at a les availants	\$1.52 si une ensur se produit sur cet élément Non Non	1-568891775-1310009993-2218789375-1104		
			Ajouter des membres Administratur BONGRANDI Adminiscal Commun Options Intercorps is traitement des éléments sur cette extension Supprimer cet élément bragui fir éat plus appliqué Appliquer une ficie en par asteppique	S-15-2 si une erreur se produit sur cet élément Non Non Non	1-568891775-1310009993-2218769375-1104		
			Ajottet das mentins Administratur BONGRANDI Admini-local Commun Options Intercompro le traitement des éléments sur cette extension Supprimer cet élément losqu'il n'est plus appliqué Appliquer une fois et ne pas réappliquer	S-1-5-2 si une ensur se produit sur cet élément Non Non	1.568891775-1310009993-2218769375-1104		
		Config	Ajonistear en mentens Administratur BONGRANDI Admin-local Commun Options Interrorpre la traitement des éléments sur cette extension Supprimer cet élément korsqu'i n' est plus apolqué Appliquer une fois et ne pas réappliquer urration utilisateur (activée)	S-1-5-1 si une eneur se produit sur cet élément Non Non Non	1.568891775-1310009993-2218769375-1104		

Afin d'uniformiser l'ensemble des postes de l'entreprise BONGRAND, j'ai mis en place une GPO imposant un fond d'écran identique pour tous les utilisateurs.

Le fond d'écran est téléchargé depuis le dossier partagé "GPO" du serveur, puis il est déployé directement sur le poste.

GPO fond écran :

🔶 🙇 🖬 🥥 📓 🖬				
Sestion de stratégie de groupe wallp	paper			
A Forêt : bongrand.local	due Détails Paramètres Délégation			
Im Domaines				
Default Domain Policy	Général			
< BONGRAND	Anting		Crier	
wallpaper	Propriétés		Creer	
Groupes	Fichier(s) source(s)		\\servdata\GPO\Fond ecran\bongrand-cie.png	
✓	Fichier de destination		C:\Windows\Web\Wallpaper\bongrand-cie.png	
Admin_Syst				
Admin Syst	Attributs		Décestivé	
Domain Controllers	Caché		Déractivé	
 Objets de stratégie de groupe 	Ambie		Déractivé	
Admin_Syst	Active		Desective	
Default Domain Controllers Policy	Commun			
Default Domain Policy wellpaper	Ontines			
Similar Filtres WMI	Options	stansion ei une arraur se produit sur cet élément	Nan	
> Digits GPO Starter	Supprimer cet élément lorsqu'il n'est plus appliqué	aenson si une eneur se procar aur cor element	Non	
🙀 Sites	Appliquer une fois et ne pas réappliquer		Qui	
👸 Modélisation de stratégie de groupe	y Abudan ana ana ana has nahir-i		ou .	
Résultats de stratégie de groupe	Configuration utilisateur (activée)			
	Stratégies			
	Modèles d'administration			
	Définitions de stratégies (fichiers ADMX) récupérées	à partir de l'ordinateur local.		
	Bureau/Bureau			
	Stratégie	Paramètre	Commentaire	
	Papier peint du Bureau	Activé		
	Nom du papier peint :		C:\Windows\Web\Wallpaper\bongrand-cie.png	
	Exemple : avec un chemin local : C\ windows	web/ wallpaper/ home.jpg		
	Exemple : avec un chemin UNC : \\Server\S	hare\Corp.ipg		
	Style du papier peint :		Centrer	
				 Accedez aux parametres pour activer windows.



Partage de fichiers

Afin de favoriser le travail collaboratif, j'ai mis en place un partage de fichiers sous Windows. Cela permet aux salariés de partager des documents, de travailler sur des dossiers communs et de gérer les droits d'accès (ACL) pour attribuer à chaque utilisateur uniquement les permissions nécessaires.

■ 🗹 📜 =		Gérer	Data (E:)	
Fichier Accueil Partage	e Affichage	Outils de lecteur		
\leftarrow \rightarrow \checkmark \uparrow \backsim \checkmark Ce	PC > Data (E:)	>		
Accès rapide	Nom	^		Modifié le
	📕 Partages			16/04/2025 20:10
	📜 Partagesin	fos\$		28/04/2025 11:33
 Telechargemer Documents 	📕 Utilisateur	s		16/04/2025 20:17

Droits sur un dossier :



.....

Documentation technique fiche nº1



Pour la gestion des ACL, seuls des groupes sont utilisés afin d'éviter de mélanger utilisateurs et groupes sur un même dossier. La nomenclature des groupes suit la structure suivante : "BONG" pour le domaine, "GS" pour Global Security, "Direction" pour le nom du dossier, et "M" pour le niveau de permission (Modification).



Documentation technique fiche n°1

PFSENSE

Mise en place des VLANs

Afin de sécuriser le réseau de l'entreprise BONGRAND, j'ai mis en place trois VLAN :

VLAN 10 - Administration : regroupe le serveur Windows Server ainsi que le poste de l'administrateur.

VLAN 20 - Bases de données : contient le serveur Debian hébergeant les bases de données ainsi que les services internes tels que Wazuh et Zabbix.

VLAN 30 - Utilisateurs : dédié aux postes clients des salariés de l'entreprise BONGRAND.

Interfaces / VLANs											
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs		
VLAN Interfaces											
Interface	VLAN tag		Priority		De	scription			Actions		
em1	10				Ad	dmin			er 💼		
em1	20				Ba	ases de don	nées		e 🖉 💼		
em1	30				Ut	ilisateurs			et 🕯		

Mise en place des règles de Pare-feu

VLAN 10

Ru	Rules (Drag to Change Order)													
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue Schedule	Description	Actions			
	~	0/6.93 MiB	*	*	*	VLAN10 Address	443 80	*	*	Anti-Lockout Rule	\$			
	~	0/0 B	IPv4 TCP	192.168.50.250	80 - 443	VLAN10 subnets	*	*	none		҄ <i>҈≵₫</i> 00 Х			
	~	0/0 B	IPv4 TCP/ UDP	VLAN10 subnets	*	192.168.10.250	53 (DNS)	*	none		҄ ₺ <i>₱</i> ©О ×			
	~	0/0 B	IPv4 TCP	VLAN30 subnets	*	192.168.10.250	445 (MS DS)	*	none	partages windows	҄ <i>҈∛</i> [] О і́п ×			
	~	0/0 B	IPv4 TCP	VLAN10 subnets	*	192.168.20.250	1514	*	none	agent wazzuh	҄ <i>҈≵∥</i> ́ []О́ і́́́а Х			
	~	0/0 B	IPv4 TCP	VLAN10 subnets	*	192.168.20.250	10051	*	none	agent zabbix	҄ ∄			
	~	0/0 B	IPv4 TCP	VLAN10 subnets	*	192.168.20.250	62354	*	none	agent glpi	҄ <i>҈∜</i> [] О і́п Х			
	~	0/0 B	IPv4 TCP	VLAN10 subnets	*	192.168.20.250	3306	*	none	bases de données	҄ ∄ ∕́ □О ́ 面 ×			
	~	0/47 KiB	IPv4 TCP	VLAN10 subnets	*	192.168.50.250	443 (HTTPS)	*	none		҄ ₺ <i>₱</i> ©О 面 ×			
	~	11/4.11 GiB	IPv4 *	VLAN10 subnets	*	*	*	*	none	Default allow LAN to any rule	ᢤ∥⊡⊘面 ×			
	~	0/0 B	IPv4 ICMP any	*	*	*	*	*	none		҈∜//́□О́п Х			



Projet E6

Documentation technique fiche nº1

• •	0/0 B	IPv6 *	VLAN10 subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	҈⊎∕⊡ Х
□ × #≡	0/640 B	IPv4 *	*	*	*	*	*	none		₺₡₽०₸

VLAN 20

Rules	Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue Scl	hedule	Description	Actions
• •	0/121.12 MiB	IPv4 TCP	192.168.20.250	*	*	80 - 443	*	none			∜৶⊄© ×
□ ✓	0/0 B	IPv4 TCP	VLAN30 subnets	*	192.168.20.250	3306	*	none		bases de données	ử∥⊡⊘≣ ×
•	0/0 B	IPv4 TCP	192.168.50.250	*	192.168.20.250	3306	*	none			ử∥⊡©面 ×
□ ✓	0/0 B	IPv4 TCP	192.168.20.250	*	192.168.50.250	3306	*	none			∜৶⊄© ×
•	0/227 KiB	IPv4 TCP	192.168.20.250	*	*	10050 - 10051	*	none			∜৶⊄©© ×
	0/0 B	IPv4 TCP	VLAN30 subnets	1514 - 1515	192.168.20.250	1514 - 1515	*	none			∜৶⊄©© ×
□ ✓	0/0 B	IPv4 TCP	192.168.50.250	1514 - 1515	192.168.20.250	1514 - 1515	*	none			∛⊉∕⊡©≣ ×
□ ✓	0/0 B	IPv4 TCP	VLAN10 subnets	1514 - 1515	192.168.20.250	1514 - 1515	*	none			∛ ⊄ © 🖻 ×
	0/428 KiB	IPv4 TCP/ UDP	192.168.20.250	*	This Firewall (self)	53 (DNS)	*	none			ঔঐ⊡⊘面 ×
□ ✓	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			∛ ∕∕ □ ⊘ লি ×
□ × #≣	0/1.12 MiB	IPv4 *	*	*	*	*	*	none			ݨ∥□╲亩

VLAN 30

Floa	ating	WAN	VLAN10 V	LAN20 VLAN3	D VLA	N50						
Rul	es (D	rag to Chan	ige Order)									
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	0/15 KiB	IPv4 TCP/UDP	VLAN30 subnets	*	VLAN10 subnets	88	*	none			҄҈ℋ ⅅ Ѻ҆҆ ҆ ҅ ӣ Ӿ
	~	0/0 B	IPv4 TCP	192.168.50.250	80 - 443	VLAN30 subnets	*	*	none			҄҈ℋ ⅅ Ѻ ӓ ×
	 Image: A start of the start of	0/5.91 MiB	IPv4 TCP/UDP	VLAN30 subnets	*	192.168.50.250	*	*	none			҈∜₽́Ѻ ѽ ×
	~	0/325 KiB	IPv4 TCP	VLAN30 subnets	*	192.168.10.250	389 (LDAP)	*	none			҄҈ℋ ⅅ Ѻ҆ ӓ ×
	 Image: A second s	4/131 KiB	IPv4 UDP	VLAN30 subnets	*	192.168.10.250	53 (DNS)	*	none			҄҈∜₽́ѺѢ́×
	 Image: A start of the start of	4/68.30 MiB	IPv4 TCP/UDP	VLAN30 subnets	*	*	443 (HTTPS)	*	none			҄҈ℋ ⅅ Ѻ҆ ӓ ×
	~	0/0 B	IPv4 TCP	VLAN30 subnets	*	192.168.50.250	443 (HTTPS)	*	none			҄҈∜₽́ѺѢ́×
	~	0/0 B	IPv4 UDP	VLAN30 subnets	*	This Firewall (self)	67 - 68	*	none			҄҈ℋ ⅅ Ѻ҆҆ ҆ ҅ ӣ Ӿ
	~	0/0 B	IPv4 TCP	VLAN30 subnets	*	192.168.20.250	3306	*	none			҄҈∜₽́Ѻ ѽ ×
	 Image: A second s	0/0 B	IPv4 TCP	VLAN30 subnets	*	192.168.20.250	10051	*	none			҄҈∜₽́Ѻ ѽ ×
	 Image: A start of the start of	0/0 B	IPv4 TCP	VLAN30 subnets	*	192.168.20.250	62354	*	none			҄҈ℋ ⅅ Ѻ҆҆ ҆ ҅ ѿ Ӿ
	~	0/108 KiB	IPv4 TCP	VLAN30 subnets	*	192.168.10.250	445 (MS DS)	*	none			҄҈∜₽́ѺѢ́×
	 Image: A second s	0/0 B	IPv4 TCP	VLAN30 subnets	*	192.168.20.250	1514	*	none			ᢤ᠕ᢆᢕᢩ᠐ᢁᢆᢣ
	~	0/3 KiB	IPv4 ICMP any	*	*	*	*	*	none			ᢤᢞ᠋ᢩ⊡⊘ <u>ਜ਼</u> ́×
	×≅	0/621 KiB	IPv4 *	*	*	*	*	*	none			ৼৢ৻৻৻৻৻



Documentation technique fiche n°1

SERVEUR DEBIAN

J'ai décidé d'installer un serveur Debian 12 afin d'y héberger les services de bases de données, Wazuh et Zabbix. J'ai choisi Debian car il s'agit d'un système d'exploitation open source, reconnu pour sa légèreté et sa fiabilité, ce qui en fait un excellent choix pour un serveur. L'installation est simple et rapide.

.....

Ce serveur est nommé "debiandatabases", il est accessible via son adresse IP en ssh avec le mot de passe : debianalexandre



Une fois notre serveur en fonctionnement, je peux installer les services nécessaires pour l'entreprise BONGRAND en commençant par Docker.

Installation Docker et Portainer

L'installation de Docker se fait directement en ligne de commande sur notre machine hôte. C'est une installation simple qui nécessite que quelques lignes de commandes.



Documentation technique fiche nº1

Une fois notre Debian mise à jour et curl d'installé, nous allons installer GPG de Docker à fin de permettre aux utilisateurs de communiqué de manière sûre avec le dépôt.

install -m 0755 -d /etc/apt/keyrings

echo \

"deb [arch=\$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/debian \ \$(. /etc/os-release && echo "\$VERSION_CODENAME") stable" | \ tee /etc/apt/sources.list.d/docker.list > /dev/null

Nous ajoutons l'adresse du dépôt Docker dans les sources.

Nous devons refaire un **apt update** car nous avons ajouté un dépôt.

Une fois cette update faite, nous pouvons lancer l'installation de Docker et Docker-compose en plugin, il nous sera utile pour créer des multi-conteneurs, tel qu'un WordPress et sa base de données.

apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin

Ajouter notre utilisateur dans le groupe Docker.

```
usermod -aG docker « utilisateur »
```

Portainer

À présent que nous avons Docker d'installé, nous pouvons installer Portainer, ce qui va nous permettre de gérer nos machines virtuelles plus facilement et grâce à une interface web.

Nous allons créer un volume Docker nommé "portainer_data" pour stocker les données de Portainer.

Docker volume create portainer_data

Lancer le conteneur Portainer.

docker run -d --name=portainer --restart=always -p 8000:8000 -p 9443:9443 -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest

Maintenant que nous avons Portainer d'installé, nous pouvons déployer des services plus simplement grâce à des stacks

			Version : A					
		Docum	Date : 25/04/20	25				
Upgrade to Business	Edition	Stacks					a odmia v	
Dortainer.id	N «	Stacks ISt 2			٩	k Search ×	Remove + Add stack II :	
🧼 local		Same↓↑ Filter ⊽	Type ↓↑ Compose	Control	Created ↓↑ 2025-03-20 20:14:12	Updated ↓↑ -	Ownership↓↑ ⊗ administrators	
 Destributed Templates Stacks 	~	homarr	Compose	Limited	2025-03-17 09:44:34		& administrators	
 ♥ Containers ∷≡ Images ♣ Networks 		zabbix	Compose	Limited 0	2025-03-12 18:47:24 2025-03-13 19:42:07		֎ administrators ֎ administrators	
Volumes Events							Items per page 10 v	
🖭 Host								
New version available Dismiss See what's r	2.27.4 New							
portainer.io Community Edit	tion 2.27.1 LTS							

Wazuh

L'installation de Wazuh a été réalisée à l'aide d'un fichier Docker-compose.yml, ce qui permet de déployer la solution en seulement cinq minutes, le temps nécessaire pour télécharger l'image.

Docker-compose.yml:

Wazuh App Copyright (C) 2017, Wazuh Inc. (License GPLv2) /ersion: '3.7'
¢ wazun App Copyright (C) 2017, wazun Inc. (License GPLV2) version: '3.7'
Version: 3.7
Services:
wazun.manager:
<pre>image: wazun/wazun-manager:4.11.1</pre>
nostname: wazun.manager
restart: always
utimits:
memlock:
SOTT: -1
nard: -1
50+T: 000300
- "1515;1515" E1/ .E1/ / =
- "514:514/udp" "EF000.EF000"
- "55000:55000"
environment:
- INDEXER_URL=NTTPS://Wazun.indexer:9200
- INDEXER_PASSWORD=SecretPassword
- FILEDEAT_SSL_VERIFICATION_NUDE-TULL
- SSL_CERTIFICATE_AUTHORITIES-/etc/sst/ruot-ca.pem
- SSL_CERTIFICATE-/etc/sst/filebeat.pem
- ADT USEDNAME-workbawa
- API_USERWANE-wazun-wui
API_PASSWORD-HySSCIS7P4301.*
- wazuh ani configuration:/var/ossec/ani/configuration
wazuh_api_configuración./var/ossec/api/configuración
wazuh_ett./var/ossec/ett
- wazuh gueue:/var/ossec/gueue
- wazuh var multigroups:/var/ossec/var/multigroups
- wazuh_integrations:/var/ossec/var/muttigroups
wazun_integracions./var/ossec/integracions

Interface web :



× + 😳 Wazuh σ \times Non sécurisé | https://wazuh.bongrand.local/app/wz-home#/overview??_g=(filters:1),refreshInterval:(pause:1; value:0),time:(from:now-24h:to:now))&_a=(filters:1),query:(language&...) C **Ø** аљ ··· 12 £≞ ... \leftarrow ≡ w. Overview a 🛛 🗇 AGENTS SUMMARY LAST 24 HOURS ALERTS Active (4) Critical severity High severity Medium severity Low severity Disconnected (1) 2 34 8,219 0 Rule level 15 or higher Rule level 12 to 14 Rule level 7 to 11 Rule level 0 to 6 ENDPOINT SECURITY THREAT INTELLIGENCE Configuration Assessment Malware Detection Threat Hunting Vulnerability Detection Scan your assets as part of a configuration assessment audit. Check indicators of compromise triggered by malware infections or Browse through your security alerts, identifying issues and threats in your Discover what applications in your environment are affected by wellcyberattacks. environment. known vulnerabilities. MITRE ATT&CK File Integrity Monitoring Explore security alerts mapped to adversary tactics and techniques for Alerts related to file changes, including permissions, content, ownership, and attributes. better threat understanding. SECURITY OPERATIONS CLOUD SECURITY 19°C Ensoleillé へ目目の

Configuration Wazuh :

ి 🗊 🕲 Wazuh	×Z	Zabbix docker: History [refreshed 🗙 🕞 Tablea	u de bord des élément	s - G 🗙 🏻 q avoir les infos windows	server gra 🗙 📘 Mo	nitoring Windows servers with	🗙 🛛 🧑 Dashboards - Grafana	× +	F	- 0 ×
← C S Non sécurisé ht	tps://wazuh.bon	grand.local/app/vulnerability-detection#/ow	erview/?tab=vuls&t	abView=dashboard&_g=(filters:l().	refreshInterval:(pause	::lt,value:0),time:(from:now-2	4h,to:now))&_a=(filters:().4	query:(language:ku	ery,query:")) as 💮 🏠	수 … 🥠
W. Vulnerability Detect	tion									a ⑦
Dashboard Inventory Ev	rents								0	Explore agent
Search									DQL	C Refresh
wazuh.cluster.name: wazuh.manager	valuated Unde	r evaluation 💿 🕀 Add filter								
2 Critical - Severity		303 High - Severity		634 Medium - Severity		20 Low - Se	b verity		558 Pending - Evaluation	
Top 5 vulnerabilities	Count	Top 5 OS		✓ Count <	Top 5 agents			✓ Count ✓	Top 5 packages	Count
CVE-2024-21096	11	Debian GNU/Linux 12 (bookworm)		1,522	debian-databases			774	linux-image-amd64	1,390
CVE-2025-3576	10	Microsoft Windows 10 Pro 10.0.19045.	5608	1	debian-web 748				vim-common	16
CVE-2024-56406	8			DESKTOP-3650259				1	vim-tiny	16
CVE-2025-0395	8								cryptography	12
CVE-2024-9681	6								libxml2	10
Most common vulnerability score			Most vulnerable	OS families			Vulnerabilities by year of	publication		
-1. 57.72 7.72 7.72 7.7 7.7 7.7 0.1 0.2 0.2 0.2 0.2 0.2 0.2 0.2 0.2	- Oug Court	\$ <u>\$</u>	dabian - ed 41 900 teop Windows -	- 190 - 190 - 190	- Occo Count	1200- 1400-	500 300 200 300 200 200 200 8 5 2 2 2018 2018 2018	Ad 9 2020 2021AC vulnerability.public	Multi-terrespondent respondent for the first state of the first state	dium w jh tical Windows.
P Taper ici pour rechercher	t	i 🕐 🗖 🛱 💁							🛃 CAC large 60 +0.59% - ヘ 🔛 0	14-29

J'ai ajouté une configuration pour que Wazuh bloque les tentatives de Brute-Force sur SSH. Configuration bloque SSH :



.....

Date : 25/04/2025

< Manager configuration



Zabbix

Idem que pour l'installation de Wazuh, Zabbix a été installé grâce à un docker-compose.yml ce qui facilite et améliore la gestion de ce service.

Docker-compose.yml:



Documentation technique fiche n°1

Date : 25/04/2025

GNU nano 7.2	docker-compose.yml
services:	
zabbix-server:	
<pre>image: \${ZABBIX_SE</pre>	RVER_IMAGE:-zabbix/zabbix-server-mysql:ubuntu-7.2.1}
container_name: za	bbix-server
restart: unless-st	topped
ports:	
- 10051:10051	
	SERVER HOST
DB SERVER PORT	3306
MYSOL USER: \${M	(SOL USER)
MYSOL_PASSWORD:	\${MYSOL_PASSWORD}
MYSQL_DATABASE:	\${MYSQL_DATABASE}
networks:	
- network-zabbi>	K
zabbix-frontend:	
image: \${ZABBIX_FF	RONTEND_IMAGE:-zabbix/zabbix-web-nginx-mysql:ubuntu-7.>
restart: unless-st	copped
container_name: fi	contend
ports:	
- "8880:8080"	
- "8443:8443"	
	STOR SERVED HOST
MYSOL USER \$ \$M	(SOL LISER)
MYSOL PASSWORD:	\${MYSOL PASSWORD}
MYSOL_DATABASE:	\${MYSOL_DATABASE}
PHP_TZ: \${TZ}	
ZBX_SERVER_HOST:	zabbix-server
ZBX_SERVER_PORT:	10051
depends_on:	
- zabbix-server	
networks:	
- network-zabbi>	
zabbix-agent:	

Interface web :



Configuration Zabbix :



Installation Base de données

Pour utiliser tous ces services, une base de données est nécessaire. J'ai choisi d'installer MariaDB directement sur le serveur, sans utiliser de conteneur Docker.

J'ai sécurisé l'installation en utilisant la commande mysql_secure_installation, ce qui m'a permis de définir un mot de passe pour accéder à la base de données.

Après l'installation de MariaDB, j'ai créé la base de données pour le service Zabbix ainsi que l'utilisateur associé. Cet utilisateur a un caractère " % " dans le champ "host", ce qui lui permet de se connecter à la base de données depuis n'importe quelle adresse IP.

