

Emetteur(s) : Saviard Matthieu Destinataire(s) : Jury BTS SIO

Date: 18/02/2024

Objet : Mise en place d'un serveur NAGIOS au sein de mon infrastructure

Nagios est un système de surveillance open source utilisé pour superviser en temps réel la disponibilité, les performances et l'état des éléments d'un environnement informatique, tels que les réseaux, les systèmes et les applications.

Il utilise des plugins pour effectuer des vérifications spécifiques et envoie des alertes en cas de détection d'anomalies, permettant aux administrateurs de réagir rapidement. Nagios offre une interface web facile d'utilisation, prend en charge la personnalisation des plugins, la planification des tâches et peut être étendu grâce à une communauté active.

Nagios XI est une version améliorée avec des fonctionnalités avancées.

1. Préréquis

Pour réaliser notre serveur Nagios, voici donc nos prérequis \rightarrow

	NAGIOS							
RAM	OS	HARD DRIVE	NECESSITE					
2GB	Debian 12	30GB	Routeur					
			DNS					

Voici la configuration reseau :

CA	CARTE RESEAUX				
ENS33 192.168.110.10					
ENS160	NAT				

La carte NAT sera retirée après l'installation du service Nagios

Nagios est utilisé principalement via son interface web. Quand les utilisateurs sont connectés, ils peuvent accéder au tableau de bord principal, qui montre les statuts des équipements réseau, des services et des applications en surveillant. L'interface permet de visualiser rapidement l'état opérationnel de chaque élément, que ce soit en termes de disponibilité, de performances ou d'éventuelles erreurs, grâce à des codes couleur faciles à comprendre.

Les sections dédiées aux "hôtes" et aux "services" offrent des détails spécifiques, des graphiques de performance et un historique des événements. Cette interface offre également des fonctionnalités de configuration, de filtrage, de recherche et de gestion des notifications, ce qui rend la surveillance, la personnalisation et la réaction rapide aux incidents plus simples. Par conséquent, l'interface web de Nagios



Voici le schéma de notre infrastructure globale →

2. Préparation de la machine et installation de nagios

a. Configuration de la machine

On commence par mettre à jour la machine

root@nagios:~# root@nagios:~# apt update && upgrade

Ensuite on met à jour le fichier resolv.conf avec notre DNS et domaine

```
GNU nano 5.4
domain localdomain
search localdomain
nameserver 192.168.32.2
```

On installe les outils DNS et la commande WGET ainsi que curl



b. Installation de Nagios

On va commencer par installer Nagios sur notre machine \rightarrow

curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh

root@nagios:~# curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh

Une fois installé, on va aller sur notre dashboard depuis une AD primaire via edge grâce à notre IP Nagios →



On va donc aller sur <u>http://192.168.110.10</u> et retirer la carte NAT qu'on avait utilisé pour l'installation

On arrive sur une page qui va nous demander de configurer nagios et de rentrer une clé pour un trial

General System Settings

Program URL	http://192.168.110.10/nagiosxi/		Ø
Timezone	(UTC+01:00) Paris	~	
Language	French (Français)		
User Interface Theme	Modern Dark	~	
	Use HTTPS only (all HTTP requests	will be redirected t	o HTTPS)

License Settings

License Type	Trial Licensed Free (Limited)
	Trial includes unlimited nodes + enterprise features. Includes access to trial support. Click to get a trial key
Trial Key	NDI5MzIwNDYxMjkxNDEy

Next >

On change le mot de passe ightarrow

- ID : nagiosadmin
- MDP: @Azerty123

Ensuite, il se connecter et accepter le contrat -> Pour pouvoir accéder au dashboard



On arrive sur le dashboard. Le dashboard sera le lieu ou nous pourrons faire la supervision de nos serveurs. En effet, dans le cadre de notre infrastructure, Nagios sera utilisé pour gérer nos serveurs, et évaluer si ils sont en surcharge ect.



On y trouve des fonctionnalités telles que :

Des fonctionnalités telles que :

- Vue d'ensemble : Statut global et graphiques récapitulatifs.
- Hôtes et Services : Liste et détails des hôtes et services surveillés.
- Cartes : Représentation visuelle de la topologie du réseau.
- Événements : Journal des événements, alertes et notifications.
- Rapports : Rapports prédéfinis et personnalisables.
- Configuration : Gestion des hôtes, services, politiques de notification.
- Planification : Horaires de vérification des hôtes et services.
- Administration : Gestion des utilisateurs, configuration système.
- Tableau de bord personnel : Personnalisation pour des besoins spécifiques.

3. Installation d'un agent Windows

Notre machine Nagios est finalement prête, nous allons donc pouvoir ensuite installer sur notre serveur AD primaire. En effet, on peut découper les agents nagios en deux parties :

- Les machines Windows
- Les machines Linux

Ici, nous allons commencer par installer sur notre serveur AD Windows

C'est lui qui va remonter les infos vers notre serveur Nagios \rightarrow

Un agent Nagios est un logiciel léger installé sur les systèmes à surveiller. Son rôle principal est de collecter des informations locales sur la santé et les performances du système, puis de les transmettre au serveur Nagios central pour une analyse approfondie. Voici un résumé de son utilité et de son fonctionnement :

→ Ici on va installer un agent de type NCPA (Nagios Cross- Platform Agent)

Un agent NCPA :

Allons donc commencer en allant sur notre machine primaire \rightarrow

Gestionn	aire de serveur 🔸 Tableau de bord 🛛 🔹 🕫 🖉 Géree	r Outils Afficher Aid
🔢 Tableau de bord	BIENVENUE DANS GESTIONNAIRE DE SERVEUR	
Serveur local Tous les serveurs	1 Configurer ce serveur local	
官 DHCP 윤 DNS ब Services de fichiers et d ▷	RAPIDE 2 Ajouter des rôles et des fonctionnalités 3 Ajouter d'autres serveurs à gérer NOUVEAUTÉS 5	
	Creer un groupe de serveurs S Connecter ce serveur aux services cloud	Masquer
	Rôles et groupes de serveurs Rôles : 4 Groupes de serveurs : 1 Nombre total de serveurs : 1 Image: AD DS 1 Image: AD DS 1	1

On va donc aller dans Gérer \rightarrow « Ajouter des rôles et fonctionnalités » \rightarrow « Installation basée sur un rôle une fonctionnalité » \rightarrow Serveurs SNMP

Dratacala DNPD	~
Proxy du service de migration du stockage	
Qualité E/S du service	
Redirecteur WebDAV	
Réplica du système de stockage	
RPC sur proxy HTTP	
Sauvegarde Windows Server	
Serveur de gestion des adresses IP (IPAM)	
Serveur SMTP	
Serveur WINS	
Service d'activation des processus Windows	
Service de migration du stockage	
Service de recherche Windows	
Service de réseau local sans fil	
Service de transfert intelligent en arrière-plan (BITS)	
 Service SMMP 	
V Fournisseur WMI SNMP	
Services TCP/IP simples	
Support de partage de fichiers SMB 1.0/CIFS	
Support Hyper-V pour Host Guardian	\sim

On va faire suivant \rightarrow Puis installer ce service

En fait, quand on installe des Outils et fonctionnalités, c'est comme si on installait des services va cette icône →



On va donc aller sur notre service installé, sur notre machine. Taper « Services » dans la barre de recherche Windows et chercher → « Service SNMP »

	Services				Propriétés de Servi	ce SNMP (Ordina	teur local)	×	
6	Fichier Action A	ffichage ?			Interruptions	Séc	urité	Dépendances	
Corbeille	⇐ ➡ 📰 🖸	2 🗟 🛛 📷 🕨 🔳 🕪			Général	Connexion	Récupération	Agent	
	🔅 Services (local)	Services (local)	Nom	Descrip	Nom du service : Nom complet :	SNMP Service SNMP			
GLPI Nouveau document te		Service SNMP Arrêter le service Redémarrer le service Description : Permet aux requêtes SNMP (Simple Network Management Protocol) d'être traitées par cet ordinateur. Si ce service est arrêté, l'ordinateur ne pourra pas traiter les requêtes SNMP. Si ce service est désactivé, tous les services qui en dépendent explicitement ne pourront pas démarrer.	Nom Service Hyper-V PowerShell Service Initiateur iSCSI de M Service Initiateur iSCSI de M Service Interface du magasi Service Liste des réseaux Service Partage réseau du L Service Partage réseau du L Service Partage réseau du L Service Portection avancée Service Protection avancée Service PushToInstall de Wi Service Serveur proxy KDC Service Serveur proxy KDC Service State Repository (St Service Synchronisation dat Service User Experience Virt Service User Experience Virt Service User Experience Virt	Descrip Fournit Gère les Ce serv Coordo Identifii Active I Partage Ce serv Le servi Surveill Offre u Le servi Le servi Permet Fournit Synchr Assure Dermet	Nom complet : Description : Chemin d'accès d C:\Windows\Syst Type de démarrag État du service : Démarrer Vous pouvez spéc service. Paramètres de dé	Service SNMP Permet aux requi Management Pro ontinutaur Gi nue les fichiers exécutat em32\snmp exe pe : Autor En cours d'exécut Antêter offier les paramètres marrage :	êtes SNMP (Simple N toco)) d'être traitées eenvise aet amêté l'e bles : natique ion Suspendre qui s'appliquent au d	Vetwork par cet vrtinstaur na V Reprendre démarrage du	
		Étendu Standard /				C	K Annule	r Appliquer	

On va donc dans Propriétés → On va cocher toutes les cases dans la rubrique Agent →

incertoptions	s Sécu	inté	Dépendances
Général	Connexion	Récupérati	on Age
es systèmes de l'indiquer la pers éseau pour cet o	gestion d'Internet peu onne contact, l'empla ordinateur.	ivent demander cement du systè	au service SNMF me et les service
Contact :			
implacement :			
Service			
Physique 🗸	Applications	Liaison de don	nées et sous-rése
<mark>∕ Int</mark> ernet	Bout en bout		

Puis ensuite nous allons aller dans \rightarrow « Sécurité »

- Dans l'onglet "Sécurité", commencez par ajouter votre communauté SNMP, dans cet exemple nommée "safetech.com", à la liste. Suivez ces étapes :
- Cliquez sur "Ajouter...".
- Définissez les droits et le nom de la communauté, par exemple, "safetech.com".

Général	Connexion	Réci	inération	Agent
Internations	S	écurité	Déne	ndances
interruptions			Бере	inddrices
Envoyer une ir	nterruption d'auth	entification		
Noms de comm	unautés accepté	s		
Communauté		Droit	s	
Configurati	on du service Sl	NMP		×
Droits de co	ommunauté :		Ajo	outer
LECTURE	ECRITURE	~	An	nuler
Nom de la o	communauté :			
nagios.safe	etech.com			
A:		1:1:	0	
Ajou	ter M	odifier	Supprimer	

→ Cochez l'option "Accepter les paquets SNMP provenant de ces hôtes".

Ensuite, ajustez la liste d'hôtes autorisés comme suit :

1) Retirer"localhost" de la liste si présente.

X Propriétés de Service SNMP (Ordinateur local) 1 Récupération Général Connexion Agent Sécurité Dépendances Interruptions Envoyer une interruption d'authentification Noms de communautés acceptés 1 Communauté Droits LECTURE ÉC... Ir nagios.safetech.com e P 5 Modifier ... Ajouter... Supprimer le r Accepter les paquets SNMP provenant de n'importe quel hôte Ti Accepter les paquets SNMP provenant de ces hôtes 0 192.168.110.10 n n 1 P Ajouter ... Modifier... Supprimer p n De OK Annuler Appliquer

Ajoutez l'adresse IP du serveur Nagios dans les serveurs autorisés

Ensuite on enregistre \rightarrow Puis on retourne sur notre dashboard Nagios

Sur le dashboard aller dans configure \rightarrow configuration wizard

On va cliquer sur cette icône et ensuite commencer à configurer notre premier agent \rightarrow



➔ On choisit Windows



Et on cherche ensuite tout en bas « Windows SNMP »



➔ On va donc ensuite rentrer les paramètres de notre machine AD primaire qu'on veut superviser

	192.168.100.2		
	L'adresse IP de la m	achine Windows que vous soul	haitez surve
Système d'exploitation:			

Paramètres SN	IMP
Spécifiez les parar	nètres utilisés pour surveiller la machine Windows via SNMP.
Version SNMP:	
	La version du protocole SNMP utilisé pour commicate avec la machine.
	vous devez utiliser snmp v1 si la langue de votre système Windows n'est pas l'anglais
Port HTTP::	
	le port snmp à utiliser, le port par défaut est le port 161.
snmp paramèt	res de version
Communauté Si	
	La chaîne de communauté SNMP utilisé pour nécessaire d'interroger la machine Windows

Faire « Next » et ensuite on va choisir les éléments lesquels ont veut superviser \rightarrow



Voici la liste des éléments que nous pouvons surveiller \rightarrow



lecteurs sélectionner un nouveau lecteur dans la liste déroulante	assistant va rempiir detecte le	clears, pour ajouter p	ius de
	cteurs selectionner un nouvea	u lecteur dans la liste	déroulante.
Conduire: C: 🗸 🛆 80 % 🕕 95 %	nduire: C: 🗸 🛕 80	% 🚺 95 %	

➔ On fait suivant

On laisse la configuration de base, avec l'agent qui enverra son statut toutes les 5 minutes

Paramètres de surveillance des
Définir les paramètres de base qui déterminent la façon dont l'hôte et de service (s) doivent être surveillés.
Dans des circonstances normales:
Surveiller l'hôte et de service (s) à chaque 5 minutes.
Lorsqu'un problème potentiel est détecté pour la première:
Vérifiez à nouveau l'hôte et de service (s) à chaque 1 minutes jusqu'à 5 fois avant <u>envoyer une notification</u> .
✓ Arrière Suivant > ✓ Terminer

On fait « terminé »

*	Services		Ð	٠	2	ii	
tat dı	u service p	our cet	hôt	e			Dernière mise à jour: 2024-02-18 03:43:
Service	2	Statut		Durée	Tentative	Dernière vérification	Informations sur l'état
CPU Usa	age 📈	Ok		N/A	1/5	2024-02-18 03:42:22	2 CPU, average load 3.5% < 80% : OK
Drive C:	: Disk Usage	Ok		N/A	1/5	2024-02-18 03:42:45	C:\Label: Serial Number 3847e2ec: 21%used(12968MB/61110MB) (<80%) : OK
Physical Usage	Memory	Pending		N/A	1/5		
Ping Pending			N/A	1/5			
Virtual I Usage	Memory	Pending		N/A	1/5		

On peut ensuite voir sur nos dashboards nos infos remonter ightarrow

On va faire la même sur notre autre serveur Windows AD Secondaire ightarrow

Au final, pour note infrastructure nous obtenons les machines suivantes \rightarrow

4. Installation d'un agent Linux

On va donc installer un agent GLPI sur une de nos machines Linux → Nous allons tout d'abord commencer par notre serveur Ubuntu Zimbra qui est une application critique pour notre infrastructure →

Comme pour Windows, nous allons devoir installer le service SNMP ightarrow

root@zimbra:~# apt install snmpd –y__

On va supprimer le contenu du fichier de configuration \rightarrow

```
oot@zimbra:~# echo "" > /etc/snmp/snmp.conf
```

Et on va ensuite le remplir de cette façon \rightarrow

```
sysLocation nagios.safetech.com
sysContact root<root@safetech.com>
agentaddress udp:161,udp:[::1]:161
rocommunity nagios.sitka.local default
```

Puis on restart le service \rightarrow

root@zimbra:~# service snmpd restart root@zimbra:~# service snmpd status
 snmpd.service – Simple Network Management Protocol (SNMP) Daemon.
Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
Active: active (running) since Sun 2024–02–18 03:12:31 UTC; 6s ago
Process: 15836 ExecStartPre=/bin/mkdir –p /var/run/agentx (code=exited, status=0/SUCCESS)
Main PID: 15837 (snmpd)
Tasks: 1 (limit: 8178)
Memory: 6.0M
CGroup: /system.slice/snmpd.service
└─15837 /usr/sbin/snmpd -LOw -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTrig
févr.18 03:12:31 zimbra.safetech.com snmpd[15837]: Cannot adopt OID in UCD–SNMP–MIB: laLoadFloat :D
févr. 18 03:12:31 zimbra.safetech.com snmpd[15837]: Cannot adopt OID in UCD–SNMP–MIB: la∟oadInt ::=>
févr.18 03:12:31 zimbra.safetech.com snmpd[15837]: Cannot adopt OID in UCD–SNMP–MIB: laConfig ::= >
févr.18 03:12:31 zimbra.safetech.com snmpd[15837]: Cannot adopt OID in UCD–SNMP–MIB: laLoad ::= { >
févr.18 03:12:31 zimbra.safetech.com snmpd[15837]: Cannot adopt OID in UCD–SNMP–MIB: laNames ::= {>
févr.18 03:12:31 zimbra.safetech.com snmpd[15837]: Cannot adopt OID in UCD–SNMP–MIB: laIndex ::= {>
févr. 18 03:12:31 zimbra.safetech.com snmpd[15837]: /etc/snmp/snmp.conf: line 1: Warning: Unknown t
févr. 18 03:12:31 zimbra.safetech.com snmpd[15837]: /etc/snmp/snmp.conf: line 2: Warning: Unknown t
févr. 18 03:12:31 zimbra.safetech.com snmpd[15837]: /etc/snmp/snmp.conf: line 3: Warning: Unknown t
févr. 18 03:12:31 zimbra.safetech.com snmpd[15837]: /etc/snmp/snmp.conf: line 4: Warning: Unknown t
lines 1-20/20 (END)

→ On vérifie que ca marche bien avec la commande suivante :

5. Installation et configuration de NCAP

Enter a password to use for the MySQL n MySQL nagiosxi Password: nagios