Mise en place de Eyes Of Network

1/6

Installation

Dans un premier temps on déploie une machine virtuelle sur laquelle on installe la distribution Eyes of Network à partir de l'image iso.

On lance l'installation du système d'exploitation



On ne teste pas la validité de notre image ISO et procédons directement à l'installation en sélectionnant *Skip*



L'étape suivante consiste à choisir la langue d'installation, ici Français. Puis nous configurerons le

périphérique de stockage en sélectionnant Périphériques de stockage basiques :



On poursuit en saisissant le nom de notre machine, **GSB-Supervision** puis cliquons sur le button *Configurer le réseau*

	Modification de S	ystem eth0	
Nom de la connexio	n : System eth0		
 Connecter autom Disponible pour t 	natiquement tous les utilisateurs		
Filaire Sécurité 80	2.1x Paramètres IP	/4 Paramètres IF	PV6
Méthode : Manu	iel		•
Adresses			
Adresse	Masque de réseau	Passerelle	Ajouter
172.25.0.20	255.255.255.0	172.25.0.253	Supprimer
Serveurs DNS :	172.25.0.	1	
Domaines de re	cherche :		
ID de client DHC	CP :		
Requiert un a	adressage IPv4 pour o	que cette connex	ion fonctionne
			Routes
		Annuler	Appliquer

Ne pas oublier de cocher la case *Connecter automatiquement* sans quoi notre machine n'auras pas de réseau au démarrage automatiquement.

Sur l'écran suivant, nous choisissons le fuseau horaire de notre machine. Il correspond à *Europe/Paris*.

On continu en saisissant le mot de passe de l'utilisateur root.

La suite consiste à choisir le type d'installation, pour nous ce sera Utiliser tout l'espace

Eichier Affighøge ⊻M				
	> ち 🖾 🕼 🕼 🔶 🚸			
	Eyes Or Network V.4			
Quel type	d'installation souhaitez-vous ?			
	Utiliser tout l'espace Supprime toutes les partitions sur le(s) périphérique(s) sélectionné(s). Cela inclut les partitions créées par d'autres systèmes d'exploitation.			
_	Astuce : Cette option supprimera les données du (ou des) périphérique(s) sélectionné(s). Assurez-vous de bien faire des copies de sauvegardes.			
0	Remplacement du (ou des) système(s) Linux existant(s) Supprime uniquement les partitions Linux (créées depuis une installation Linux précédente). Ceci ne supprimera pas les autres partitions que vous pourriez avoir sur votre (ou vos) périphérique(s) de stockage (tel que VFAT ou FAT32).			
_	Astuce : Cette option supprimera les données du (ou des) périphérique(s) sélectionné(s). Assurez-vous de bien faire des copies de sauvegarde.			
Réduire la taille du système actuel Réduire les partitions existantes afin de créer de l'espace pour le partitionnement par défaut.				
0	Utiliser l'espace libre Conserve vos données et partitions actuelles et n'utilise que l'espace non-partitionné sur le(s) périphérique(s) sélectionné(s), en supposant que vous possédez suffisamment d'espace disponible.			
0	Créer un partitionnement personnalisé Créer manuellement votre propre partitionnement personnalisé sur le(s) périphérique(s) sélectionné(s) à l'aide de l'outil de partitionnement.			
Chiffrer Revoir	le système et modifier le schéma de partitionnement			
	Reversion Précédent Suivant			

Sur la page suivante, nous cochons *Personnaliser maintenant* afin de faire le choix des logiciels à installer.

Après avoir effectuer toute ces opérations, nous sommes maintenant prêt à lancer l'installation d'Eyes of Network.

Configuration

Community

Nous modifions la communauté en remplaçant la valeur par défaut par **gsbppe**. On clique sur l'onglet *administration* puis configuration du menu *Nagios*. On sélectionne ensuite *Nagios Resources* et on rentre notre nom de communauté dans le champs *\$USER2\$*. On valide en cliquant sur le bouton *Update Resource Configuration*.

On poursuit dans le menu snmp de *Généralités*. On remplace la ligne com2sec notConfigUser default EyesOfNetwork par com2sec notConfigUser default gsbppe. On valide en cliquant sur le bouton *update*.

On passe dans le menu *snmptrapd* en changeant authCommunity log, execute, net EyesOfNetwork par authCommunity log, execute, net gsbppe.

On applique ensuite les configuration grâce au menu *appliquer la configuration* de *nagios* dans lequel on clique sur le bouton *Restart*.

On termine par un redémarrage des services : processus de Généralités puis restart.

Mail

Nous avons configurer des comptes utilisateurs avec nos adresses mail au préalable. Les templates intégrant le group *admins*, assigné à nos utilisateurs, pour les notifications des différents services nous n'avons aucune autre manipulation à faire de ce coter.

Nous devons configurer le serveur postfix local (installer avec EON) en tant que relais SMTP en éditant le fichier **/etc/postfix/main.cf**. On recherche les lignes concernant les *relayhost* et y ajoutons le notre comme suit :

relayhost = [192.168.222.85]

On redémarre ensuite le service :

service postfix restart

Notre serveur peut maintenant envoyer des mails.

Jeu d'essai

Situation	Opération(s) réalisée(s)	Résultat
Connexion snmp entre EON et une machine	On utilise l'option snmpwalk dans EON	On obtiens un résumé du snmpwalk dans la fenêtre active si la connexion fonctionne. cf. capture 1
Passage à l'état critique du serveur web 1	On coupe l'interface du serveur web 1.	Le serveur 2 web reprend la main pour l'applicatif. Dans l'onglet disponibilité on observe le changement d'état du serveur web 1 en critique pour le service interfaces
Réception d'un mail en cas de problème	Suite au problème créer précédemment on regarde si un mail a été envoyer.	On obtiens un mail suite au problème créer

Capture 1

TEST SNMP	
HOST NAME / IP :	NOET - 172 39 6 10
172.29.0.10	16031 1 1 2 2 2 4 0 1 0
SNMP COMMUNETY :	snmpwalk -c gsbppe -v 2c 172.29.0.10
gsbppe	
	SNMPv2-MIB::sysDescr.0 = STRING: Linux GS8-Web 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u6 x86_64
SNMP VERSION (SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
version 20 💌	ELSMAN-EVENT-MEDISystep i metristance = Timeticks: (120010) 0:21:20.10
	SIMPV2-MD:SYLCHIACCO = STRING: PH SIMPV2-MIR-services = STRING: CSR-Web
Run It 1	SNMPy2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Bay
Prodet and a	SNMPv2-MIB::svsServices.0 = INTEGER: 72
	SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
	SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
	SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
	SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SH-MIB::usmMIBCompliance
	SMMPV2-MIB::sysORID.4 = OID: SMMPV2-MIB::snmpMIB
	SNMPV2-MIB::sysORID.5 = OID: TCP-MIB::ccpMIB
	SNMP 2 MIB - SNS RIDA = ODD I P MID-NP
	SNMP2-MIB::ever0810.8 = 010: SNMP-V/EW-BASED-ACM-MIB::vacmBasicGroup
	SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
	SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
	SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
	SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
	SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
	SNMPv2-MB isysORDescr.6 = STRING: The MB module for managing IP and ICMP implementations
	SNMPV2-MUBIISySORDESC.7 = STRINGT The MUB module for managing UDP implementations
	SNMPV2/MUBIIsySORDESC/8 = STRIMAT View-Dased Access Control Model for SNMP.
	SNMPV2-MB-H3950RUPTIME1 = Interticks (0) 0000000
	SNMPy2-MIBUSySORUpTime.3 = Timeticks: (0) 0:00:00.00
	SNMPv2-MIB::sysORUpTime.4 = Timeticks: (1) 0:00:00.01
	SNMPv2-MIB::sysORUpTime.5 = Timeticks: (1) 0:00:00.01
	SNMPv2-MIB::sysORUpTime.6 = Timeticks: (1) 0:00:00.01
	SNMPv2-MIB::sysORUpTime.7 = Timeticks: (1) 0:00:00.01
	SNMPV2-MIB::sysORUpTime.8 = Timeticks: (1) 0:00:00.01
	IF-MIB:://Number.0 = INTEGER: 3

Capture 2

GSB-Web1	🙀 👌 interfaces		15:48:42	0d 0h 1m 12s	1/4	(Service Check Timed Out)	
	memory	ОК	15:46:11	0d 0h 31m 43s	1/4	Ram : 15%, Swap : 0% :: OK	
	partitions	ОК	15:46:49	0d 0h 31m 5s	1/4	All selected storages (~90%) : OK	
	processor	ок	15:47:27	0d 0h 30m 27s	1/4	CPU used 1.0% (<80) : OK	
	systime	OK	15:48:04	0d 0h 29m 50s	1/4	System Time OK - 12-16-2015, 15:50:39	
	uptime	CRITICAL	15:48:42	0d 0h 1m 12s	1/4	(Service Check Timed Out)	
	vmware_tools		15:49:20	0d 0h 0m 34s	1/4	ERROR: Process name table : No response from remote host '172.29.0.10'.	

Capture 3

Host DOWN alert for GSB-Web1! Boite de réception x

+	nagios Á moi ⊾
	***** Nagios *****
	Notification Type: PROBLEM Host: GSB-Web1

Host: GSB-Web1 State: DOWN Address: 172.29.0.10 Info: (Host Check Timed Out)

Date/Time: Wed Dec 16 15:50:00 CET 2015

From: https://wiki.viper61.fr/ - **Viper61's Wiki**

Permanent link: https://wiki.viper61.fr/sio/ppe3_2/g2/supervision_install

Last update: 18/09/2016 02:54