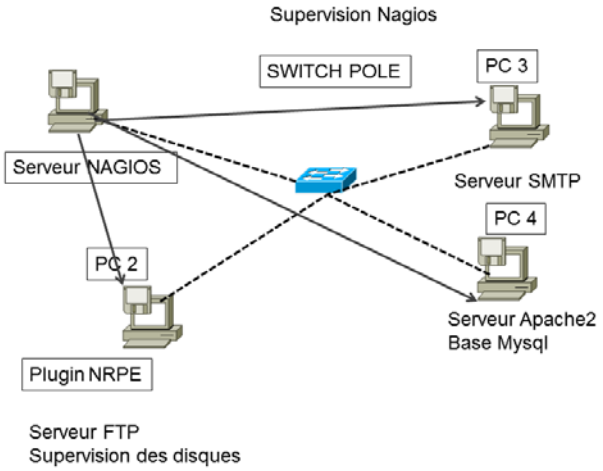
Monitoring des services avec Nagios



L'objectif de cette partie est de configurer un serveur Nagios Maitre (https://wiki.monitoring-fr.org/nagios/start, download : https://www.nagios.com/solutions/windows-monitoring/), et trois autres serveurs qui héberges des services. Nagios n'est plus forcément d'actualité, et il cependant essentiel de pratiquer la mise en œuvre de ce type d'outil. Les installations sont plus faciles sous Linux et je vous conseille de rester dans ce cadre-là. Pour les étudiants ayant des ordinateurs portables, vous pouvez configurer le client Nagios (https://wiki.monitoring-fr.org/nagios/nagios-nsclient-host) Pour avoir accès au client en mode NRPE, il faut installer les plugins sur le serveur, et évidemment sur le client (PC2).

Exercice du TP. Monitorer les services.

Quelques commandes pour vérifier le fonctionnement du client Nsclient++. En supposant que le mot de passe que vous avez choisis est « password = public » lors de l'installation du client Nsclient++, vérifier afin de faire fonctionner correctement les éléments suivants.

Sous windows, C:\Program Files\NSClient++, fichier nsclient.ini à modifier pour autoriser des accès

Charge CPU des 5 dernières minutes	**Vérification de l'espace disque C :**
• ./check_nt -H 192.168.162.15 -p 12489 -v CPULOAD -w 80 -c 90 -l 5,80,90,10,80,90 -s public	• ./check_nt -H 192.168.162.15 -p 12489 -v USEDDISKSPACE -w 80 -c 90 -l C -s public

Pour que cela soit automatisé sous Nagios, dans le répertoire /etc/nagios3 (si version 3), regardez les configurations des fichiers hosts.cfg, services.cfg, etc..
Exemple

define command{	define host{	define service{
command_name check_http	use generic-host	use generic-service
command_line $USER1$/check_http -I	host_name monserveur_http	host_name monserveur_http

$HOSTADDRESS$ $ARG1$ }	alias Serveur Web address 192.168.0.100 }	service_description HTTP check_command check_http }

Exemple serveur Mysql

- Création de l'utilisateur nagios sur la base cible
  mysql> create database nagios ;
  mysql> GRANT ALL ON nagios.* TO nagiosuser@ identified by " ;
  mysql> flush privileges ;
- Verifier que le plugin fonctionne à partir du serveur nagios
  nagios % check_mysql -P 3306 -u nagiosuser -p" -H
- Définir le service et le serveur dans les fichiers de configuration de Nagios

define command{
• command_name check_mysql
• command_line $USER1$/check_mysql -H $HOSTADDRESS$ -P $ARG1$ -u $ARG2$ -p'$ARG3$'
}
	define service{
	• use local-service
	• hostgroup_name mysql-servers
	• service_description MYSQL
	• check_command check_mysql!3306!nagiosuser!MOTDEPASSE!
	• contact_groups mysql-services
	}
		define host{
		• host_name monhost
		• use mongroupe_primaire
		• hostgroups mysql-servers
		• check_period prod-period
		• address @IP
		}

Exemple de configuration pour check_nt

Fichier command.cfg

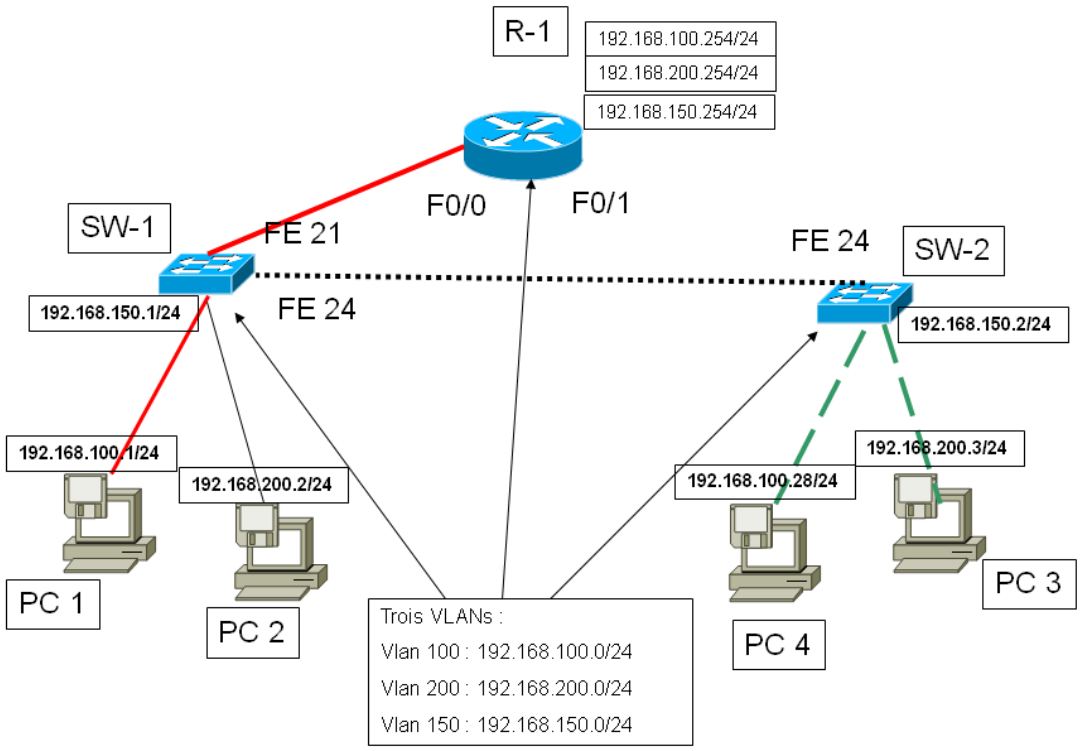
define command {
command_name check_nt
command_line $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s public -v $ARG1$ $ARG2$
}
	define service {
	use generic-service
	host_name seven-manu
	service_description CPU Load
	check_command check_nt!CPULOAD!-l 5,80,90
	}

define service {
use generic-service
host_name seven-manu
service_description Memory Usage
check_command check_nt!MEMUSE!-w 80 -c 90
}
	define service {
	use generic-service
	host_name seven-manu
	service_description Explorer
	check_command check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
	}
		define service {
		use generic-service
		host_name seven-manu
		service_description C:\ Drive Space
		check_command check_nt!USEDDISKSPACE!-l c -w 80 -c 90
		}

Installation du server NRPE sur le serveur à monitorer (voir https://blog.nicolargo.com/2007/10/surveiller-vos-serveurs-linux-avec-nagios-et-nrpe.html) apt-get install nagios-nrpe-server nagios-plugins	Côté serveur nagios

/etc/nagios/nrpe.cfg
allowed_hosts=127.0.0.1,@IP
debug=1
	./check_nrpe -H 137.121.162.28 -c check_load
	OK - Charge moyenne: 0.15, 0.62, 0.69|load1=0.150;15.000;30.000;0;
	load5=0.620;10.000;25.000;0;
	load15=0.690;5.000;20.000;0;

Schéma du réseau à mettre en œuvre par pôle



Un routeur, deux SW, 4 PC, 3 vlans 100,200, et adm 150

Questions

1) **Mettre en œuvre ce réseau : routeurs, management**
   - configurer le routeur et vérifier que les IP sont accessibles
   - configurer le VLAN 150 sur tous les équipements actifs. Vérifier que toutes les IP du vlan 150 sont accessibles.

2) **Brancher et configurer les postes**
   - Configurer les VLAN 100 et 200
   - Configurer les PCS. Vous pouvez mettre plus de PC, plus de switches, si vous le souhaitez

   PC1 : ip 192.168.100.1/24 - trouver la GW associée
   PC2 : ip 192.168.200.2/24 - trouver la GW associée
   configurer le SW1 en fonction des adresses IP de PC1 et PC2

   PC3 ip 192.168.200.3/24 – trouver la GW associée
   PC4 ip 192.168.100.4/24 – trouver la GW associée (si vous ajoutez un PC)
   faire la configuration de SW2

   - Vérifier le ping de tout le réseau

3) **Mettre un serveur Cacti + Mysql + apache2** (voir http://doc.ubuntu-fr.org/cacti)

- Configurez le serveur Cacti sur le VLAN 200
- Monitorer tous les équipements actifs
- Générez du trafic en utilisant MZ (http://www.perihel.at/sec/mz/mzguide.html#udp) ou IPERF! Que constatez-vous ?

4) Administration SNMP

- Utiliser les commandes SNMP pour récupérer manuellement la liste des interfaces du routeur. Idem sur les switches.
- Utilisez la commande SNMP appropriée pour éteindre un port de switch. Vérifiez que vous avez le bon nom de communauté SNMP définit dans la configuration des switches.
- Récupérer la table de routage du routeur en SNMP

5) Serveur DHCP

- Installer et configurer un serveur DHCP sur le serveur Cacti
- Configurer le routeur pour que les requêtes DHCP d'un autre réseau puissent joindre le réseau du serveur DHCP (par exemple, situé dans le VLAN 200).
- Basculer une machine du VLAN 100 en DHCP pour vérifier que celle-ci récupère bien une adresse IP.
- Cherchez les bons paramètres qui devraient vous permettre de configurer le réseau et le serveur DHCP pour faire fonctionner le PXE

6) Capture de trafic

- Mettez en œuvre le port mirroring sur un switch et capturez le trafic avec wireshark

7) Bouclage

- Entre le SW1 et le SW2 branchez un câble réseau supplémentaire sur les interfaces FA0/23 de chacun des switches. Vérifiez avant cela que les interfaces FA0/23 ne sont pas configurées.
- Que se passe-t-il ?
- Configurer les interfaces FA0/23 avec tous les Vlans. Que se passe-t-il ?

8) Sécurisation

- Afin que seules quelques machines puissent avoir accès au vlan d'administration, mettez l'ACL qui convient sur le routeur, pour que seuls les postes du vlan 100 puissent y avoir accès.
- Que se passe-t-il pour votre serveur Cacti. Comment devez-vous changez l'ACL sur le routeur pour que le monitoring se fasse encore.