A. Concepts généraux avec SNMP

1. Que signifie l'acronyme SNMP ?

SNMP : Simple Network Management Protocol

2. Citer les cinq aires fonctionnelles de la supervision, avec un exemple d'application pour chacune d'elles (env. 0,5 page au total).

FCAPS

Gestion de Fautes : consiste à détecter, isoler et corriger des opérations anormales, généralement à partir d'évènements générés par le réseau.

Gestion de Configuration : consiste à identifier, collecter et fournir des données de configuration aux entités managées en garantissant la continuité de leur service d'intercommunication des services.

Gestion de la Comptabilité (Accounting) : consiste à évaluer le coût d'utilisation des ressources managées

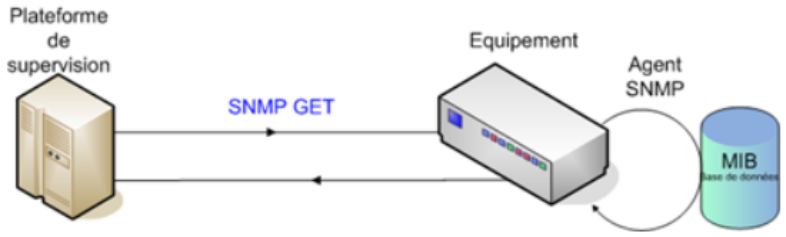
Gestion de Performances : consiste à évaluer le comportement des ressources managées et le test des activités de communication

Gestion de la Sécurité : consiste à assurer la sécurité du réseau et à protéger les ressources managées.

3. Illustrer le fonctionnement du protocole SNMP au travers d'un schéma, en représentant les différentes interactions entre un gestionnaire et ses agents (env. 0,75 page au total).

Le principe de SNMP : sur chacune des machines, on installe un petit programme : l'agent SNMP. Cet agent enregistre en permanence des informations relatives à la machine. Il stocke ces informations dans une base de données appelée MIB (Management Information Base).

Le schéma ci-dessous illustre le principe de fonctionnement du protocol SNMP :



Le manager va interroger l'agent grâce à la requête SNMP GET. L'agent (il gère les informations relatives à l'équipement) va fouiller dans la MIB pour positionner ou donner la valeur demandée. Puis l'agent va lui-même remonter l'information au manager via une trap snmp. Si par exemple une carte réseau tombe, l'agent pourra en informer le manager sans que celui-ci en ait fait la demande.

4. Définir à quoi correspondent les acronymes ASN.1, SMI et MIB ? Puis exprimer la relation entre SNMP et ces trois termes en quelques lignes.

ASN.1 : Abstract Syntax Notation 1
SMI : Structure of Management Information
MIB : Management Information Base

Le protocole SNMP utilise une base d'informations de gestion (MIB) de structure hiérarchique pour définir la signification et le type d'une valeur déterminée.
Le SMI est l'ensemble de règles pour identifier d'une manière unique les objets gérés. Il définit la structure logique de la base informationnelle MIB(Management Information Base). La MIB est la base de données des informations de gestion maintenue par l'agent SNMP, auprès de laquelle le manager va venir pour s'informer. Un fichier MIB est un document texte écrit en langage ASN.1 qui décrit les variables, les tables et les alarmes gérées au sein d'une MIB.

5. Expliquer à quoi correspondent les quatre primitives SNMP suivantes : TRAP, INFORM, GET et GETNEXT. Parmi celles-ci, indiquer celles qui sont pull-based.

GET : Opération permettant de demander une ou plusieurs variable
GETNEXT : permet de demander le nom et la valeur de la prochaine variable de la MIB (ce qui est utile pour découvrir les attributs d'une MIB, ou itérer sur un tableau);
GETBULK : permet de récupérer plusieurs variables consécutives en une requête. Elle permet ainsi d'améliorer les performances.
SET : permet d'assigner une valeur sur un objet
TRAP : demande à l'agent de signaler un événement (par exemple: linkdown, authentication failure, etc.), mais n'attend pas d'acquittement du gestionnaire, ce qui en fait une opération non fiable.
INFORM : spécifique à SNMPv2, cette opération améliore Trap en acquittant en plus la bonne réception de la notification.

Les primitives qui sont pull-based : GET, GETNEXT, GETBULK

B. Monitoring avec Nagios

6. Sous Nagios, expliquer comment sont implantés les tests et comment leurs résultats sont transmis à la plateforme.

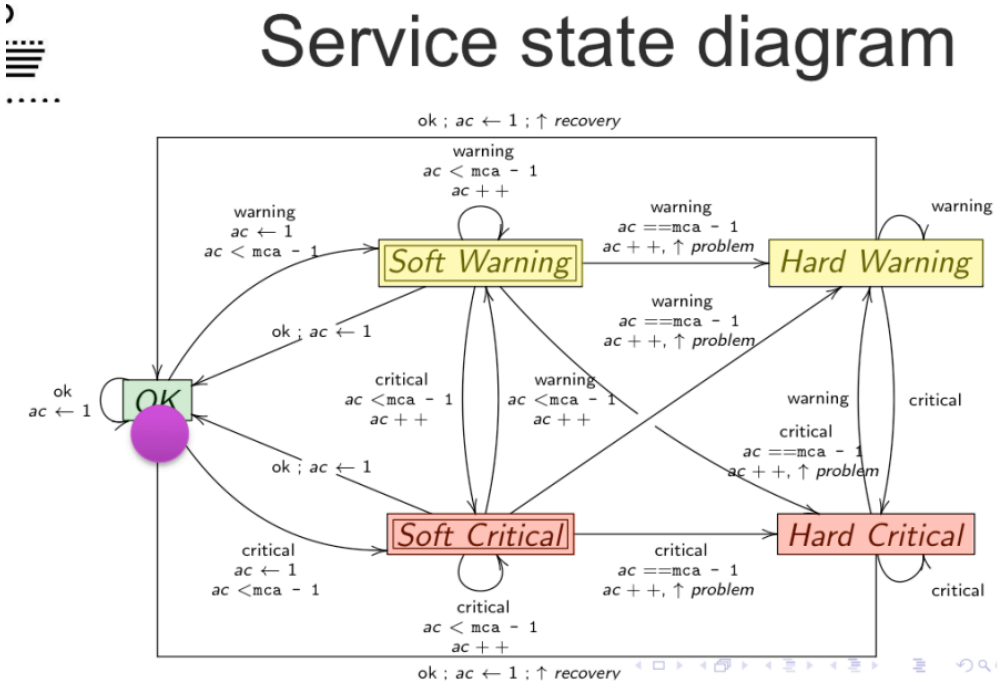
Les tests sont exécutés périodiquement par le serveur Nagios, afin d'inférer l'état des services. Un test est implanté à l'aide d'un plugin, et un plugin correspond typiquement à une commande ou un script, qui est exécuté sur un équipement. La transmission des résultats se fait par le protocole ICMP.

7. Proposer un script shell correspondant à un plugin Nagios permettant de lever une alerte en fonction du nombre de processus sur une machine Linux. Vous pouvez utiliser la commande "ps -e | wc -l" pour connaître le nombre de processus, avec comme résultat un état WARNING dès que l'on dépasse 100 processus, et un état CRITICAL dès que l'on dépasse 150 processus.

check_procs -w 100 -c 200

```
#!/bin/bash
process = ‘ps -e | wc -l’
if [ $process  -lt 100 ]
then
        exit 0
else if [ $process  -lt 150 ]
        then
                exit 1
        else
                exit 2
        fi
fi
```

8. Sous Nagios, quels sont les états possibles pour un service ? Expliquer comment est calculé l’état d’un service. Vous vous aiderez d’un schéma représentant le diagramme d’état d’un service, en indiquant les différentes conditions de transition (notamment ac (attempt count) et mca (maximum check attempt)) (env. 1 page au total).

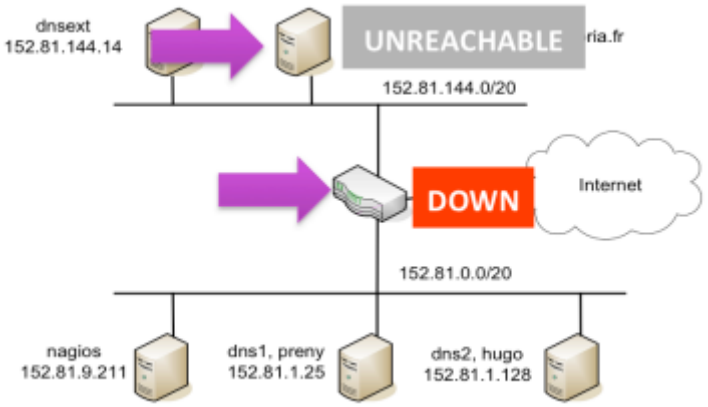


9. Sous Nagios, expliquer les trois principales catégories de tests distants qui peuvent être utilisées, et en quoi elles diffèrent.

- Direct Network Checks : protocoles réseau, exécutés par le serveur Nagios
- Tests SSH : utilisation d’un plugin dédié (check_by_ssh), nécessite d’avoir les droits en exécution sur la machine distante.
- NRPE (Nagios Remote Plugin Executor) : plugins préconfigurés sur la machine distante.

10. Sous Nagios, expliquer à quoi correspond l’escalade de notifications, et illustrer votre propos à l’aide d’un exemple.

L'objectif est de fournir un support multi-niveaux pour la résolution de problèmes, en s'appuyant surune hiérarchie des contacts et groupes de contacts. Cette hiérarchie peut reposer sur le niveau de technicité, le niveau de responsabilité, ou plus simplement la localisation géographique des contacts.



Routeur : parent serveur web si en panne, si état routeur = OK alors le serveur web est bien en panne. Sinon, le routeur est à l'état down et serveur web inatteignable, donc Unreachable

11. Indiquer les différentes étapes nécessaires pour configurer Nagios de sorte à surveiller que la page principale d'un site web n'est pas défacée (par exemple, changement d'une image suite à une attaque).

Il faut utiliser le Website Defacement Wizard de l'interface Nagios.
Paramétrer l'URL du site Web à surveiller.
On peut ensuite paramétrer le type de défaçage à contrôler : mots clefs dans une liste, liste de mots prédéfinies, position des images, …

C. Instrumentation avec JMX (Java Management eXtention)

12. Quels sont les services fournis par un agent JMX ?

- ➢ Management applet (m-let) : permet le chargement et l'instanciation dynamique de classes en utilisant une url dédiée qui pointe sur un fichier utilisant des tags particuliers pour décrire les MBeans à traiter.
- ➢ Moniteur : permet d'observer les modifications de valeurs de propriétés numériques ou chaîne de caractères d'un MBean et de notifier ces changements à des abonnés.
- ➢ Timer : permet l'envoi de notifications répétitives ou programmées selon une valeur temporelle à des abonnés en vue de l'exécution de traitements.
- ➢ Relations entre MBeans : permet de définir et de maintenir des associations entre MBeans et d'assurer l'intégrité de ces relations.

Ces services peuvent être implémentés sous la forme de MBeans ce qui leur permet d'être utilisés par les autres MBeans et d'être administrables.

13. Dans le modèle de notifications JMX, expliquer comment est réalisé le filtrage.

NotificationFilter (IF) qui, associé à une souscription, permet de savoir si une notification passe un filtre avant émission. Le filtre est évalué par la méthode notificationEnabled.

14. Quels modèles de déploiement JMX permettent de gérer le cycle de vie d'une application Java instrumentée ?
Le component model est utilisé pour gérer le cycle de vie d'une application.

15. Quand et comment sont définies les opérations de gestion d'un MBean dynamique ?
Les opérations de gestion d'un MBean dynamique sont générées à l'exécution par l'objet de supervision. Elles sont définies dynamiquement par l'objet de supervision.

16. Que retourne l'instruction ManagementFactory.getPlatformMBeanServer() ?
Elle retourne un objet de type MBeanServer
`(MBeanServer mbs = ManagementFactory.getPlatformMBeanServer();)`

D. Evolution des protocoles de gestion

17. Comparer les protocoles de gestion NetConf et SNMP, en détaillant les différences et similitudes entre deux protocoles. Vous synthétiserez votre analyse dans un tableau comparatif, où vous indiquerez clairement les critères choisis.

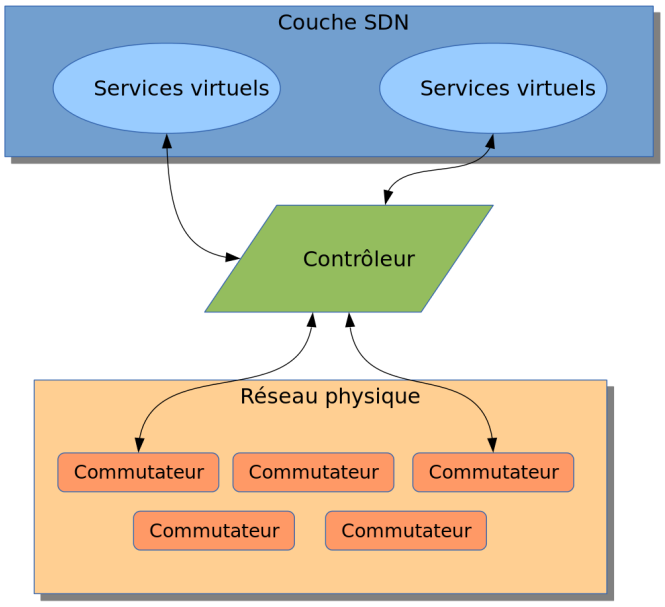
	SNMP	NETCONF
Protocol de transport	UDP	SSH / TCP
Langage	SMI	Yang
Standard	IETF	IETF
Send event notification	YES	YES
Ressources	OID	Chemins
Configuration changes	No	Yes
Encodage	JSON	XML

18. En quoi consiste le monitoring de flux ? Comment est représenté un flux réseau ? Expliquer le cycle de vie d'un flow record avec NetFlow

- Traffic monitoring
  - Collect statistics about traffic forwarded through the network
  - Different from monitoring device states

19. A quoi correspond un réseau logiciel (software-defined network) ? Illustrer son fonctionnement à l'aide d'un schéma montrant les composants et leurs intéractions.

SDN est un modèle d'architecture réseau qui permet aux administrateurs de réseaux de gérer les services de réseaux par abstraction de fonctionnalités.



…

20. Soit la table de flux OpenFlow ci-dessous, décrire les différents champs de la table, puis déduire à quoi peuvent correspondre les différentes entrées (comportement du commutateur (switch) programmable).

Port	Src MAC	Dst MAC	VLAN ID	Priority	EtherType	Src IP	Dst IP	IP Proto	IP ToS	Src L4 Port ICMP Type	Dst L4 Port ICMP Code	Action	Counter
*	*	0A:C8:*	*	*	*	*	*	*	*	*	*	Port 1	102
*	*	*	*	*	*	*	192.168.*.*	*	*	*	*	Port 2	202
*	*	*	*	*	*	*	*	*	*	21	21	Drop	420
*	*	*	*	*	*	*	*	0x806	*	*	*	Local	444
*	*	*	*	*	*	*	*	0x1*	*	*	*	Controller	1

…

GLHF tout le monde