AROC

Examen final

Analyse réseau

Pour vérifier le temps de réponse/la latence réseau entre votre machine et une autre machine sur le réseau, peut-on utiliser la commande **PING** ?

A. Oui
B. Non

Pour suivre le chemin que suit un paquet depuis votre machine à une autre machine, pouvez-vous utiliser la commande netstat ?

A. Oui
B. Non

Pour voir toutes les interfaces IPv4 qui écoutent sur votre machine, quelle commande utiliser ?

A. lsof -i
B. netstat
C. lsof
D. netstat 127.0.0.1
E. ping localhost

Surveillance et gestion réseau

La surveillance et la gestion des réseaux couvre les thèmes suivants:

A. Détecter les problèmes dans le réseau quand ils apparaissent
B. Observer des tendances et comportements pour aider à planifier l'expansion de votre réseau et des resources associées, si il y a besoin
C. Générer des alertes automatiquement quand des problèmes apparaissent
D. Savoir concevoir une base SQL correctement formée.
E. Aider à respecter les obligations de garantie de service (SLA) envers vos clients.

Quel logiciel sera mieux en mesure d'illustrer les variation de gigue sur votre réseau ou services ?

A. Smokeping
B. Nagios
C. Cacti
D. RANCID
E. NetFlow

Peut-on mesurer la place disque sur une machine distante avec l'aide de Cacti ?

A. Oui
B. Non

Quel logiciel peut-on utiliser pour détecter qu'un routeur est “mort” ou injoignable ?

A. Cacti
B. Smokeping
C. Nagios
D. Swatch
E. All of the above

Que signifie SNMP ?

A. Simple Network Management Protocol

B. Service for Network Management Project
C. Simple NetBios Management Protocol
D. Simplified Network Monitoring Protocol
E. Serious New Measuring Project

Est-ce que la communication peut-être chiffrée en SNMPv2c ?

A. Oui
B. Non

Quelle différence entre SNMP v2c et v3 ?

A. Le type d'authentification utilisée et la possibilité de chiffrer.
B. Les types d'informations retournées par les équipements SNMP
C. Aucun des choix ci-dessus.

Dans la version 3 de SNMP, vous pouvez protéger...

A. L'authentification avec utilisateur et mot de passe en utilisant un mot de passe et une fonction de hachage telle que MD5 ou SHA
B. Les données retournées en chiffrant avec DES
C. Les deux choix ci-dessus sont possibles.

IPERF peut servir à contrôler la bande passante disponible entre deux points

A. Oui
B. Non

Un système de gestion de “tickets” (incidents) est utile parce que:

A. Il sert de base de connaissance sur les problèmes passés
B. Il garde une trace de la communication avec le client du début à la fin.
C. Il peut alerter automatiquement les techniciens lorsqu'un problème est détecté par les systèmes de surveillance
D. On peut visualiser des tendances pour planifier les évolutions du réseau
E. Toutes réponses ci-dessus

Peut-on utiliser NetFlow pour localiser la source d'une attaque ?

A. Oui
B. Non

NetFlow ne fonctionne qu'avec les routeurs Cisco

A. Oui
B. Non

Un “flux de données” est défini comme étant une séquence de paquets unidirectionnelle ayant les propriétés suivantes:

A) La même adresse IP source et destination
Le même identifiant de protocole de couche 3
Le même port source et destination
Le même octet de Type de Service (QoS)
The same input interface index (ifindex)

➔ LA QUESTION CONTINUE SUR LA PAGE SUIVANTE

B) Même adresse IP source et destination
Même numéro de protocole de niveau 3
Même port source et destination
Même version du protocole SNMP

C) Même octet de type de service
Même interface de provenance (selon ifIndex)
Le même processeur est utilisé
Même taille de paquet et de MTU

Choisir la réponse correcte ci-dessus.

The program Mailgate pour RT permet à Cacti, Nagios, Smokeping et autres programmes de créer automatiquement des tickets d'incident:

A. Oui
B. Non

Est-ce que rancid peut préciser qui a commis une erreur lors d'un changement de la configuration d'un routeur ?

A. Oui
B. Non

Est-ce que SWATCH (Simple log WATcher) sait faire:

A. Alerter si un utilisateur particulier se connecte à un routeur via SSH/telnet?
B. Calculer le temps de traitement des paquets en sortie de l'interface?
C. Mesurer la gigue entre deux équipements sur le réseau ?
D. Vous réveiller avant que quelqu'un lance une attaque en déni de service contre votre réseau
E. Calculer la bande passante maximale utilisée par un de vos clients?

Les 3 lignes suivantes de configuration sur un Cisco ont quel résultat ?

```
logging 10.0.0.8
logging facility local6
logging trap errors
```

A. Envoyer les messages syslog à 10.0.0.8, catégorie local6, de priorité “error” (level 3)
B. Envoyer les messages syslog à 10.0.0.8, catégorie local6, de priorité “error” (3) et inférieurs (niveau 3 → 7)
C. Envoyer les messages syslog à 10.0.0.8, catégorie local6, de priorité “error” (3) et supéieurs (niveau 3 → 0)

Quelle commande SNMP peut on utiliser pour obtenir toutes les valeurs pour tous les OIDs disponibles sur un équipement qui implémente SNMP ?

A. snmpwalk
B. snmpstatus
C. snmpget
D. snmpset
E. snmptrap