ADMINISTRER SON RESEAU INFORMATIQUE SOUS WINDOWS SERVEUR

PROGRAMME (24H)

1) GENERALITE SUR L'ADMINISTRATION DES RESEAUX INFORMATIQUES
2) LA VIRTUALISATION
3) INSTALLATION DE WINDOWS SERVEUR
4) LES OUTILS NATIFS D'ADMINISTRATION SOUS WINDOWS
5) INSTALLATION ET CONFIGURATION DES SERVICES DE WINDOWS SERVEUR
6) TP SUR LES SERVICES DE WINDOWS SERVEUR.

Manageur de réseaux, Responsable de réseaux, Gestionnaire de réseaux

- L'administrateur réseaux est chargé de la gestion des comptes et des machines du réseau informatique d'une organisation
- L'administration de réseau est une discipline de l'informatique qui peut s'étendre à la téléphonie.
- L'administrateur réseau est également administrateur système,
- L'administrateur gère les postes de travail et les serveurs de l'entreprise.

Manager réseaux, Responsable de réseaux, Gestionnaire de réseaux

- L'administrateur réseaux est chargé de la gestion, des comptes et des machines du réseau informatique d'une organisation
- L'administration de réseau est une discipline de l'informatique qui peut s'étendre à la téléphonie.
- L'administrateur réseau est également administrateur système,
- L'administrateur gère les postes de travail et les serveurs de l'entreprise.

Lieux d’exercice et statuts

- Intervient dès la conception du réseau ou sur un réseau déjà en place.
- Appartient à la direction de l'exploitation, à la direction informatique, à une équipe de supervision du réseau ou exerce sous la responsabilité d'un directeur technique.
- Collabore étroitement avec les ingénieurs systèmes et réseaux et avec le responsable télécoms ou exploitation
- Est soumis à des astreintes, soirs et week-ends (banques, hôpitaux).

Activités et tâches

Activité 1

- Conception de l'architecture du réseau

Tâches

- Prévoir les accès simultanés au(x) serveur(s) ;
- Prévoir le volume de données maximum pouvant circuler sur le réseau ;
- Trouver le compromis entre sécurité du réseau et convivialité d'utilisation ;
- Sélectionner le matériel à utiliser ;
- Prévoir une redondance des matériels critiques.

Activité 2

- Veille à la sécurité pour l'accès aux données de l'entreprise

Tâches

- Mettre en place les pares feux et règles de sécurité nécessaires ;
- Créer des alertes et des comptes rendus ;
- Sensibiliser les utilisateurs aux risques et règles de sécurité.

Activité 3

- Support technique

Tâches

- Optimiser le temps nécessaire au transfert de compétences ;
- Réaliser des documents de présentation et des formations sur l'utilisation du réseau ;
- Assister les utilisateurs rencontrant des soucis liés au réseau ;
- Analyser l'origine des dysfonctionnements.

Activité 4

- Maintenance permanente du réseau

Tâches

- Créer des tableaux de bord pour veiller à la bonne marche du réseau et des serveurs ;
- Prévoir les montées en charge du réseau ;
- Tester la compatibilité des nouveaux équipements susceptibles d'être connectés au réseau ;
- Planifier les évolutions ou remplacements nécessaires à apporter au réseau ou aux serveurs.

Activité 5

- Veille technologique

Tâches

- Evolution des solutions réseaux et systèmes existants ;
- Evolution des normes existantes IEEE (Institute of Electrical and Electronics Engineers);
- Nouvelles normes IEEE ;
- Nouvelles solutions techniques ;
- Nouveaux outils.

Activité 6

- Compétences

Savoirs

- Compréhension des contraintes du projet :
- Délais,
- Budget,
- Fonctionnalités attendues.
- Connaissance des réseaux LAN, WAN, MAN.

Savoir faire

- Maîtriser les langages utilisés pour la mise en place d'un réseau :
- Protocoles de communication IEEE,
- Modèle OSI,
- Normes réseaux,
- Systèmes d'exploitation (Windows, Unix).
- Résoudre les problèmes détectés sur un site :
  - Trouver l'origine des problèmes,
  - Effectuer les corrections nécessaires,
  - Mettre en ligne ces corrections sans interrompre le fonctionnement du site.
- Comprendre les différents métiers de l'entreprise.
- Obéir aux normes et procédures de sécurité.

Savoir être

- Rigueur et Méthode ;
- Capacité d'adaptation ;
- Aptitude d'écoute et de dialogue (capacité de vulgarisation) ;
- Capacité à travailler en équipe.

NB : Un administrateur doit témoigner d'une grande rigueur et d'une faculté d'analyse développée.
Il doit être Autonome.
C'est avec rapidité et sang-froid que l'administrateur doit réagir face aux différents incidents liés au réseau.

OUTILS système et réseau "natifs"

- ipconfig (Windows) / ifconfig (Linux)
- traceroute (Linux) / tracert (Windows)
- ping
- arp -a
- netstat
- etherfind
- snoop
- nslookup
- Host
- Dig

IFCONFIG (LINUX) / IPCONFIG (WINDOWS)

- **ifconfig** est une commande Unix/Linux qui permet de configurer et d'afficher les informations des interfaces réseaux IP à partir de l'interpréteur de commande (adresse IP, MAC).

Sous les systèmes UNIX/Linux, la commande est la suivante:

ifconfig [-a][-au][-ad]

-*a* affiche toutes les interfaces,

-*au* celles actives et

-*ad* celles inactives.

- Sous les systèmes Windows, la commande devient :

ipconfig /all

PING (PACKET **IN**TERNET **G**ROPER)

- ping fonctionne sous Windows et sous Linux.

C'est la commande la plus utilisée pour diagnostiquer des problèmes.
Elle permet de tester la connectivité d'un ordinateur distant, en lui envoyant des paquets d'écho ICMP (Internet Control Message Protocol).
Si l'ordinateur répond au ping, c'est qu'il est joignable et, par conséquent, que la connexion réseau n'a physiquement aucun problème.

PING (PACKET INTERNET GROPER)

Ainsi pour vérifier qu'un réseau local est bien constitué, il faut "pinger" chaque ordinateur et voir s'ils répondent.
Exemple : Pour deux PC en réseau, un premier à l'adresse IP 192.168.1.12 et un second à l'adresse IP 192.168.1.108.
Pratique :

1) Lancer "cmd"
2) ping nom.de.la.machine

- nom.de.la.machine représente l'adresse IP de la machine ou bien son nom.

Résultat d'une commande ping

- Suivant le système d'exploitation, l'affichage de la sortie d'une commande *ping* pourra être légèrement différent.
- Voici le résultat d'une telle commande sous un système GNU/Linux :

ping www.commentcamarche.fr
PING www.commentcamarche.fr (163.5.255.85): 56 data bytes
64 bytes from 163.5.255.85: icmp_seq=0 ttl=56 time=7.7 ms
64 bytes from 163.5.255.85: icmp_seq=1 ttl=56 time=6.0 ms
64 bytes from 163.5.255.85: icmp_seq=2 ttl=56 time=5.5 ms
64 bytes from 163.5.255.85: icmp_seq=3 ttl=56 time=6.0 ms
64 bytes from 163.5.255.85: icmp_seq=4 ttl=56 time=5.3 ms
64 bytes from 163.5.255.85: icmp_seq=5 ttl=56 time=5.6 ms
64 bytes from 163.5.255.85: icmp_seq=6 ttl=56 time=7.0 ms
64 bytes from 163.5.255.85: icmp_seq=7 ttl=56 time=6.0 ms
--- www.commentcamarche.fr ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 5.3/6.1/7.7 ms

Résultat d'une commande ping

- Voici le résultat d'une telle commande sous un système Windows :
  - ***ping www.commentcamarche.fr***
    Envoi d'une requête 'ping' sur www.commentcamarche.fr [163.5.255.85]
    avec 32 octets de données :
    Réponse de 163.5.255.85 : octets=32 temps=34 ms TTL=54
    Réponse de 163.5.255.85 : octets=32 temps=37 ms TTL=54
    Réponse de 163.5.255.85 : octets=32 temps=32 ms TTL=54
    Réponse de 163.5.255.85 : octets=32 temps=33 ms TTL=54
    Statistiques Ping pour 163.5.255.85 :
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
    Minimum = 32ms, Maximum = 37ms, Moyenne = 34ms

```
C:\Users\N'DRIKONAN>ping www.google.ci

Envoi d'une requête 'ping' sur www.google.ci [216.58.208.163] avec 32 octets de données :
Réponse de 216.58.208.163 : octets=32 temps=551 ms TTL=52
Réponse de 216.58.208.163 : octets=32 temps=560 ms TTL=52
Réponse de 216.58.208.163 : octets=32 temps=315 ms TTL=52
Réponse de 216.58.208.163 : octets=32 temps=289 ms TTL=52

Statistiques Ping pour 216.58.208.163:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 289ms, Maximum = 560ms, Moyenne = 428ms
```

Résultat d'une commande ping

- La sortie de la commande *ping* permet ainsi de connaître :

-L'**adresse IP** correspondant au nom de la machine distante ;
-Le **numéro de séquence** ICMP ;
-La **durée de vie** du paquet (*TTL*, *Time To Live*).

La durée de vie (TTL) permet de connaître le nombre de routeurs traversés par le paquet lors de l'échange entre les deux machines.
Chaque paquet IP possède un champ TTL positionné à une valeur relativement grande.
A chaque passage d'un routeur, le champ est décrémenté.
S'il arrive que le champ arrive à zéro, le routeur interprétera que le paquet tourne en boucle et le détruira ;

Résultat d'une commande ping

-Le **temps de propagation en boucle** (*round-trip delay*) correspond à la durée en millisecondes d'un aller-retour entre la machine source et la machine cible. Un paquet doit en règle générale posséder un temps de propagation inférieur à 200 ms ;

Résultat d'une commande ping

- Le **nombre de paquets perdus**.

- Pourcentage de paquets perdus est élevé
- Temps de réponse est bas
- Les paquets arrivent dans le désordre

Conséquences : Problème matériel (Carte réseau, Câble, Connecteurs).

NB :
Sur un réseau local le temps de parcours doit être presque nul et il ne devrait pas y avoir de paquets perdus.

ARP (Address Resolution Protocol)

La commande arp permet de visualiser ou modifier la table du cache ARP d'une interface.
Elle donne la correspondance entre *une adresse IP et une adresse MAC*.
Le cache ARP de l'interface est mis à jour à chaque nouvelle requête.

-ARP -a permet d'afficher le cache de votre ordinateur.

-ARP -s 192.168.1.35 00-d0-cf-05-60-54 ajoute une entrée statique à la table.

-ARP -d vide le cache.

Traceroute

- Traceroute est similaire à l'utilitaire PING, mais fournit davantage d'informations. Le programme Traceroute surveille le chemin emprunté par un paquet jusqu'à sa destination.

Traceroute est une commande qui permet de connaître la liste des routeurs traversés lorsqu'on veut atteindre une machine distante.

- Sous les systèmes UNIX/Linux, on tape :

  traceroute nom.de.la.machine

- Sous les systèmes Windows, on tape :

  tracert nom.de.la.machine

Traceroute

```
C:\WINDOWS\system32>tracert 192.168.1.101

Détermination de l’itinéraire vers Epervier [192.168.1.101]
avec un maximum de 30 sauts :

  1    <1 ms    <1 ms    <1 ms  Epervier [192.168.1.101]

Itinéraire déterminé.
```

Nslookup (Name System Look Up)

Nslookup fonctionne sous Windows et sous Linux
Nslookup est un outil qui permet d'interroger un serveur de noms afin d'obtenir les informations concernant un domaine ou un hôte.
C'est aussi outil de diagnostic des éventuels problèmes de configuration du DNS.
nslookup affiche le nom et l'adresse IP du serveur de noms primaire et affiche une invite de commande pour l'interrogation.

- *nslookup hostname*

Nslookup (Name System Look Up)

Par défaut la commande nslookup interroge le serveur de noms primaire configuré sur la machine. On peut aussi interroger un serveur de noms spécifique en le spécifiant avec la suite de la commande précédé du signe "-":

- *nslookup host.name -serveur.de.nom*
- *L'option -r permet de lire les tables de routage.*

Nslookup (Name System Look Up)

```
C:\WINDOWS\system32>nslookup
Serveur par dÚfaut :   Air3G
Address:  192.168.1.254

>
>
C:\WINDOWS\system32>nslookup air3g
Serveur :   Air3G
Address:  192.168.1.254

Nom :    air3g
Address:  192.168.1.254
```

Netstat

- suivant les options utilisées, netstat permet de visualiser trois types d'informations :

-la première délivre les sockets valides utilisés par les différents protocoles ;

-la seconde est une des nombreuses structures de données du réseau ;

-la troisième sont des statistiques sur la transmission de paquets.

Netstat

- ~> netstat -i

```
~> netstat -i
Name  Mtu  Net/Dest   Address    Ipkts     Ierrs  Opkts    Oerrs  Collis  Queue
le0  1500  imag-batb  imag       8864760   6      8418838  2      258930  0
lo0  1536  loopback   localhost  765048    0      765048   0      0       0
~>
```

L'option -i permet de visualiser l'interface avec le réseau et les statistiques sur les paquets transmis.

~> netstat –nr

```
Routing tables
Destination Gateway Flags Refcnt Use Interface
127.0.0.1 127.0.0.1 UH 17 188811 lo0
129.88.56.0 129.88.32.156 UG 2 7866 le0
default 129.88.32.254 UG 40 579209 le0
129.88.120.0 129.88.32.254 UG 0 15984 le0
129.88.40.0 129.88.32.29 UG 2 42546 le0
```

Netstat

```
C:\WINDOWS\system32>netstat -a

Connexions actives

  Proto  Adresse locale          Adresse distante        État
  TCP    0.0.0.0:135             cracksmind:0            LISTENING
  TCP    0.0.0.0:445             cracksmind:0            LISTENING
  TCP    0.0.0.0:3389            cracksmind:0            LISTENING
  TCP    0.0.0.0:3580            cracksmind:0            LISTENING
  TCP    0.0.0.0:5040            cracksmind:0            LISTENING
  TCP    0.0.0.0:5357            cracksmind:0            LISTENING
  TCP    0.0.0.0:49664           cracksmind:0            LISTENING
  TCP    0.0.0.0:49665           cracksmind:0            LISTENING
  TCP    0.0.0.0:49666           cracksmind:0            LISTENING
  UDP      [::]:3702                  *:*
  UDP      [::]:5353                  *:*
  UDP      [::]:5355                  *:*
  UDP      [::]:53212                 *:*
  UDP      [::]:54652                 *:*
  UDP      [::]:58197                 *:*
  UDP      [::1]:1900                 *:*
  UDP      [::1]:5353                 *:*
  UDP      [::1]:59532                *:*
  UDP      [fe80::c42:419b:ace1:d7f4%14]:1900   *:*
  UDP      [fe80::c42:419b:ace1:d7f4%14]:59531  *:*
  UDP      [fe80::255a:789f:7a20:122f%13]:1900  *:*
  UDP      [fe80::255a:789f:7a20:122f%13]:59530  *:*
```

Netcut (www.arcai.com/netcut/)

- **Netcut,** est un programme qui dispose d'une interface graphique intuitive qui est compatible avec différents protocoles comme par exemple le protocole ARP.
- **NetCut** permet de :

-Détecter les utilisateurs qui sont connectés à un réseau par IP, adresse physique ou MAC et le nom du dispositif...

-Administrer tout le réseau avec un protocole ARP.

-Cloner des adresses.

-Établir des mesures de sécurité pour vous protéger des attaques.