Gestion et supervision des réseaux

Éléments de base de la configuration des équipements Cisco

Thèmes

- Modes CLI
- Accès à la configuration
- Configuration de base (nom d'hôte et DNS)
- Authentification et autorisation (AAA)
- Collecte des journaux
- Synchronisation temporelle (Date / fuseau horaire)
- Configuration SNMP
- Protocole CDP (Cisco Discovery Protocol)

Modes CLI

- Mode utilisateur EXEC
  - Accès limité au routeur
  - Peut afficher des informations mais ne peut pas visualiser ni modifier la configuration

```
rtr>
```

- Mode privilégié EXEC
  - Visualisation totale de l'état du routeur, dépannage, modification de la configuration, etc.

```
rtr> enable
rtr#
```

Accès au routeur

- Avant la mise en place de SSH
  - telnet 10.10.0.x
  - login “cisco” et “cisco” (utilisateur et mdp.)
- L'utilisateur privilégié peut passer en mode privilégié :
  - `rtr>enable  (mot de passe par défaut : “cisco”)`
  - `rtr#configure terminal`
  - `rtr(config)#`
- Saisissez des commandes de configuration
- Quittez et enregistrez la nouvelle configuration
  - `rtr(config)#exit`
  - `rtr#write memory`

Accès à la configuration

- Il y a deux configurations :
  - *Running config* est la configuration active sur le routeur
    - Stockée dans la RAM (sera perdue en cas de redémarrage du routeur)

```
rtr# configure terminal     (conf t)
rtr(config)# end
rtr# show running-config
```

  - *Startup config (config de démarrage)*
    - Stockée dans la NVRAM (RAM non volatile)

```
rtr# copy running-config startup-config  (ou)
rtr# write memory          (wr mem)
rtr# show startup-config    (sh start)
```

Configuration de base (nom d'hôte et DNS)

- Attribuez un nom
  - `rtr(config)# hostname rtrX`
- Attribuez un domaine
  - `rtr(config)# ip domain-name ws.nsrc.org`
- Attribuez un serveur DNS
  - `rtr(config)# ip name-server 10.10.0.254`
- Ou, désactivez la résolution DNS
  - `rtr(config)# no ip domain-lookup`

  L'absence de dns est *très utile* pour éviter les attentes prolongées

Authentification et autorisation

- Configurez les mots de passe de la manière la plus sûre.
  - Utilisez la méthode améliorée faisant appel à la fonction de hachage

    - Exemple :

```
# enable secret 0 cisco
# user admin secret 0 cisco
```

Authentification et autorisation

Configuration de SSH avec une clé a 2048 bits (au moins 768 pour les clients OpenSSH)

```
rtr(config)# aaa new-model
rtr(config)# crypto key generate rsa  (invite taille de clé)
```

Vérifiez la création des clés:

```
rtr# show crypto key mypubkey rsa
```

Journalisation des évènements. Forcer l'utilisation de SSH v2 :

```
rtr(config)# ip ssh logging events
rtr(config)# ip ssh version 2
```

Utiliser SSH, désactiver *telnet* (n'utiliser telnet qu'en dernier recours!)

```
rtr(config)# line vty 0 4
rtr(config)# transport input ssh
```

Note: Sur CatOS, il faut explicitement désactiver telnet…

Collecte des journaux (syslog)

- Envoyez les journaux au serveur *syslog* :

```
rtr(config)#logging 10.10.x.x
```

- Identifiez le canal qui sera utilisé (local0 à local7):

```
rtr(config)#logging facility local5
```

- Jusqu'à quel niveau de priorité souhaitez-vous enregistrer ?

```
rtr(config)# logging trap <logging_level>
```

<0-7>	**Niveau de gravité des messages de journalisation**	
Urgences	Système indisponible	(gravité=0)
Alertes	Action immédiate requise	(gravité=1)
critique	Conditions critiques	(gravité=2)
erreurs	Conditions d'erreur	(gravité=3)
avertissements	Conditions d'avertissement	(gravité=4)
notifications	Conditions normales mais importantes	(gravité=5)
informatifs	Messages informatifs	(gravité=6)
débogage	Messages de débogage	(gravité=7)

Synchronisation

Il est essentiel que tous les périphériques de notre réseau soient synchronisés à une horloge

En mode config :

```
rtr(config)# ntp server pool.ntp.org
rtr(config)# clock timezone <timezone>
```

Pour utiliser l'heure UTC

```
rtr(config)# no clock timezone
```

Si votre site applique l'heure d'été, vous pouvez procéder comme indiqué ci-dessous :

```
rtr(config)# clock summer-time recurring last Sun Mar 2:00 last Sun Oct  3:00
```

Vérifiez

```
# show clock
      22:30:27.598 UTC Tue Feb 15 2011
# show ntp status
       Clock is synchronized, stratum 3, reference is 4.79.132.217
       nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**18
       reference time is D002CE85.D35E87B9 (11:21:09.825 CMT Tue Aug 3 2010)
       clock offset is 2.5939 msec, root delay is 109.73 msec
       root dispersion is 39.40 msec, peer dispersion is 2.20 msec
```

Configuration SNMP

- Démarrez avec SNMP version 2
  - C'est plus facile à configurer et à comprendre
  - Exemple :

```
rtr(config)#snmp-server community NetManage ro 99
r10(config)#access-list 99 permit 10.10.0.0 0.0.0.255
```

Contrôle de la configuration SNMP

- Avec une machine Linux (après installation des utilitaires snmp), essayez :

```
snmpwalk -v2c -c NetManage 10.10.X.254 sysDescr
```

Configuration du protocole CDP (Cisco Discovery Protocol)

- Activé par défaut sur la plupart des routeurs modernes
- S'il n'est pas activé :

```
rtr(config)# cdp enable
rtr(config)# cdp run
```

(dans les versions plus anciennes de l'IOS de CISCO)

- Pour voir les voisins existants :

```
# show cdp neighbors
```

- Outils permettant de visualiser/afficher les annonces CDP :
  - tcpdump
  - cdpr
  - wireshark
  - tshark

Activation de NetFlow (export flux traffic)

Configurer FastExthernet 0/0 pour que soit exportés les flux NetFlow vers 10.10.0.250 sur le port 9996:

```
rtr# configure terminal
rtr(config)# interface FastEthernet 0/0
rtr(config-if)# ip flow ingress
rtr(config-if)# ip flow egress
rtr(config-if)# exit
rtr(config-if)# ip flow-export destination 10.10.0.250 9996
rtr(config-if)# ip flow-export version 5
rtr(config-if)# ip flow-cache timeout active 5
```

Ceci découpe les flux de longue durée en fragments de 5 minutes. On peut choisir n'importe quelle valeur entre 1 et 60. Laissez à 30 minutes si vos rapports de traffic ont de gros pics.

Acitvation de NetFlow (suite)

```
rtr(config)# snmp-server ifindex persist
```

Ceci active la permanence des index d'interface (ifIndex), afin que les interfaces aient toujours le même numéro dans les tables après un reboot du routeur.

On va ensuite activer les statistiques sur les gros "parleurs" (consommateurs) du réseau

```
rtr(config)#ip flow-top-talkers
rtr(config-flow-top-talkers)#top 20
rtr(config-flow-top-talkers)#sort-by bytes
rtr(config-flow-top-talkers)#end
```

On vérifie ce qu'on a fait

```
rtr# show ip flow export
rt# show ip cache flow
```

Voir les "top-talkers" (gros consommateurs) de réseau

```
rtr# show ip flow top-talkers
```

Questions?

?

For more information, check out
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html