2025.10.29 - Bloc 2 - 1 - Centraliser les journaux avec Syslog et synchroniser le temps avec NTP

Cisco Packet Tracer avec Timothee pour Bloc 1 le mercredi 29 octobre 2025 en distanciel

Centraliser les journaux avec Syslog et synchroniser le temps avec NTP

L'enquêteur et l'horloger du réseau

Imaginez que vous enquêtez sur un incident de sécurité. Vous interrogez plusieurs témoins (vos équipements réseau). Le premier vous dit : « J'ai vu une porte s'ouvrir à 10h02 ». Le deuxième dit : « J'ai vu quelqu'un de suspect à 15h30 ». Le troisième : « J'ai entendu un bruit à 02h15 du matin ». Leurs témoignages sont inutiles car leurs montres ne sont pas à la même heure !

C'est le problème que résout le duo NTP/Syslog :

- **NTP (Network Time Protocol)** est l'**horloger** du réseau. Son unique rôle est de s'assurer que tous les équipements partagent exactement la même heure, à la milliseconde près.
- **Syslog** est l'**enquêteur**. Il collecte tous les journaux d'événements (les « témoignages ») de tous les équipements et les stocke en un seul endroit sécurisé : le serveur Syslog.

En synchronisant l'heure avec NTP **avant** d'envoyer les logs à Syslog, on s'assure de pouvoir corréler les événements et de reconstituer une chronologie fiable d'un incident.

Objectifs

À la fin de ce laboratoire, vous serez capable de :

- Expliquer les rôles respectifs des serveurs NTP et Syslog.
- Activer et configurer les services NTP et Syslog sur un serveur Packet Tracer.
- Configurer un routeur Cisco comme client NTP pour synchroniser son horloge.
- Configurer le même routeur pour envoyer ses journaux d'événements à un serveur Syslog central.
- Générer des événements et vérifier leur apparition sur le serveur Syslog avec un horodatage correct.

🧩 Étape 1 : Préparation du laboratoire

Objectif :
Mettre en place la topologie de base du réseau avant la configuration des services NTP et Syslog.
Cette étape permet de vérifier la connectivité entre le routeur et le serveur, afin d'assurer la communication entre les équipements du futur réseau.

1️⃣ Ajout des équipements

Matériel utilisé :

- 1 Routeur Cisco **2911**, nommé **R1**
- 1 Commutateur Cisco **2960-24TT**, nommé **Switch0**
- 1 Serveur, nommé **LOG-SRV**

🧠 *Rôle des équipements :*

- Le **routeur R1** assure la passerelle et la configuration réseau.
- Le **commutateur Switch0** relie les différents équipements du réseau local.
- Le **serveur LOG-SRV** hébergera les services **NTP** (synchronisation de l'heure) et **Syslog** (centralisation des journaux).

2️⃣ Câblage de la topologie

Connexions à réaliser :

- **LOG-SRV (Fa0) → Switch0 (Fa0/1)**
- **R1 (GigabitEthernet0/0) → Switch0 (Fa0/2)**

Type de câble :
👉 Câble cuivre droit (*Copper Straight-Through*).

Schéma logique de la topologie :

```
R1 (G0/0) ── Switch0 (Fa0/2 ⇔ Fa0/1) ── LOG-SRV (Fa0)
```

3️⃣ Plan d'adressage IP

Équipement	Interface	Adresse IP	Masque	Passerelle par défaut
LOG-SRV	FastEthernet0	192.168.1.100	255.255.255.0	192.168.1.1
R1	GigabitEthernet0/0	192.168.1.1	255.255.255.0	—

4️⃣ Configuration des adresses IP

🖥️ Serveur LOG-SRV

1. Cliquer sur le serveur → **onglet Config**
2. Sélectionner **FastEthernet0**
3. Renseigner :

   `IP Address: 192.168.1.100 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1`
4. Vérifier que l'interface est **activée (On)**.
5. Contrôler avec la commande :

   `ipconfig`

🌐 Routeur R1

Configuration de l'interface G0/0 :

```
`R1> enable
`R1# configure terminal
`R1(config)# interface gigabitEthernet0/0
`R1(config-if)# ip address 192.168.1.1 255.255.255.0
`R1(config-if)# no shutdown
`R1(config-if)# exit
`R1(config)# end`
```

Vérification de l'état de l'interface :

`R1# show ip interface brief`

Résultat attendu :

`Gig0/0 192.168.1.1 YES manual up up`

5️⃣ Test de connectivité

Depuis le routeur :

```
R1# ping 192.168.1.100
```

✅ **Résultat attendu :**

```
Success rate is 100 percent
```

Cela confirme que la connectivité entre le routeur et le serveur est fonctionnelle.

🧠 Points à retenir (utile pour l'examen)

- Toujours **vérifier la connectivité** avant de configurer des services (ping indispensable).
- Le **câble droit** s'utilise entre des équipements de type différent.
- La **passerelle par défaut du serveur** doit pointer vers le routeur (192.168.1.1).
- Ne jamais oublier la commande `no shutdown` sur les interfaces du routeur.

⚙️ Étape 2 : Configuration du serveur et du routeur

Partie 1 — Configuration du serveur LOG-SRV

Objectif :
Configurer le serveur LOG-SRV pour qu'il fournisse deux services essentiels :

- **NTP (Network Time Protocol)** : permet de synchroniser l'heure de tous les équipements du réseau.
- **Syslog** : centralise les journaux (logs) envoyés par les équipements du réseau.

Ces deux services sont indispensables pour garantir une traçabilité fiable des événements réseau.

🔧 1️⃣ Configuration de base du serveur

a) Adresse IP du serveur

L'adresse IP a déjà été définie lors de l'Étape 1, mais il est important de la vérifier :

Interface	Adresse IP	Masque	Passerelle par défaut
Fa0	192.168.1.100	255.255.255.0	192.168.1.1

Vérification :

- Cliquer sur le serveur **LOG-SRV**
- Onglet **Config** → **FastEthernet0**
- Vérifier que l'adresse IP et la passerelle sont correctes et que l'interface est **activée (On)**

🕗 b) Activation du service NTP (Network Time Protocol)

1. Cliquer sur le serveur **LOG-SRV**
2. Aller dans l'onglet **Services**
3. Dans la liste à gauche, sélectionner **NTP**
4. Vérifier que le service est **On**
5. Ne pas activer l'authentification (elle n'est pas utilisée dans cette initiation)
6. L'heure affichée dans cette section correspond à **l'heure de référence du réseau**, c'est celle que les autres équipements (comme le routeur R1) viendront synchroniser.

"Pasted image 20251029105633.png" ne peut être trouvé.

🧠 *Rappel :*
Le protocole **NTP** fonctionne en mode client/serveur. Ici, le **serveur LOG-SRV** joue le rôle du serveur de temps.
Tous les autres équipements deviendront des **clients NTP**.

📜 c) Activation du service Syslog

1. Toujours dans l'onglet **Services**
2. Sélectionner **Syslog** dans la colonne de gauche
3. Vérifier que le service est **On**
4. La table des journaux (en bas de la fenêtre) est pour l'instant **vide** :
   ➜ elle se remplira automatiquement lorsque le routeur commencera à envoyer ses logs.

"Pasted image 20251029105841.png" ne peut être trouvé.

🧠 *Rappel :*
Le service **Syslog** centralise les messages d'événements envoyés par les routeurs, switches, serveurs, etc.
Cela permet d'avoir un **historique unique** et **fiable** des incidents réseau.

💡 Points importants à retenir

- Le **serveur LOG-SRV** joue ici un double rôle : **serveur NTP** et **serveur Syslog**.

- Tous les équipements du réseau doivent avoir **la même heure** pour corréler correctement les événements.
- En sécurité, la **cohérence temporelle** est essentielle : sans heure synchronisée, les logs perdent leur valeur d'analyse.

Partie 2 — Configuration du routeur R1

Objectif :
Configurer le routeur R1 pour qu'il se synchronise avec le serveur NTP et qu'il envoie ses journaux d'événements au serveur Syslog LOG-SRV.
Cette configuration permet au routeur d'avoir l'heure exacte et de centraliser ses logs sur un serveur externe.

🔧 1️⃣ Vérifications préalables

Avant toute configuration, il faut s'assurer que :

- L'interface **GigabitEthernet0/0** du routeur est configurée et activée.
- Le routeur peut communiquer avec le serveur LOG-SRV (ping réussi vers 192.168.1.100).

Test de connectivité :

```
R1# ping 192.168.1.100
```

✅ Si le ping fonctionne, tu peux passer à la suite.

🕒 2️⃣ Vérification de l'heure actuelle du routeur

Avant la synchronisation, le routeur affiche une heure **incorrecte** (par défaut, il démarre en 1993) :

```
R1# show clock *00:02:18.327 UTC Mon Mar 1 1993
```

🧠 *Remarque :*
C'est tout à fait normal — le routeur n'a pas de pile interne (comme une horloge de PC). Il doit donc interroger un serveur NTP pour obtenir la bonne heure.

⚙️ 3️⃣ Configuration du client NTP et Syslog

Entre en mode de configuration globale et saisis les commandes suivantes :

```
R1> enable R1# configure terminal ! Configuration du client NTP (prioritaire)
R1(config)# ntp server 192.168.1.100 ! Configuration du client Syslog R1(config)#
logging host 192.168.1.100 R1(config)# end
```

🧠 Explications techniques :

- `ntp server 192.168.1.100` → indique au routeur que le serveur LOG-SRV (192.168.1.100) est le **serveur de temps de référence**.
  ➜ Cela permettra au routeur de synchroniser son horloge automatiquement.
- `logging host 192.168.1.100` → indique au routeur **où envoyer ses journaux d'événements**.
  ➜ Tous les messages système et événements d'interfaces seront transmis au serveur Syslog.

✅ 4️⃣ Vérification rapide

Une fois la configuration faite, tu peux vérifier :

- L'heure avant/après synchronisation : `R1# show clock`
- Le serveur NTP associé : `R1# show ntp associations`

💡 Points importants à retenir

- Le **NTP** est toujours configuré **avant Syslog**, car il faut que l'horloge soit juste avant d'envoyer des journaux.
- En examen, pense à vérifier l'heure du routeur avec `show clock`.
- Une bonne pratique consiste à centraliser les logs sur un **serveur Syslog dédié** pour sécuriser les traces des équipements réseau.
- Ces configurations sont **basiques mais essentielles** dans toute architecture professionnelle.

🧩 Étape 3 : Vérification des services

Partie 1 — Vérifier la synchronisation NTP

Objectif :
S'assurer que le routeur **R1** s'est bien synchronisé avec le serveur de temps **LOG-SRV** grâce au protocole **NTP (Network Time Protocol)**.
Cette synchronisation garantit que tous les équipements du réseau partagent la même heure exacte, indispensable pour l'analyse des journaux et des incidents de sécurité.

⏱️ 1️⃣ Vérification de l'état de la synchronisation

La synchronisation NTP n'est **pas instantanée**.
Elle peut prendre **1 à 2 minutes** avant que le routeur ajuste son horloge selon celle du serveur LOG-SRV.

Commande à exécuter sur le routeur :

```
R1# show ntp associations
```

🔍 **Interprétation du résultat :**

- Au début, il est normal de ne rien voir ou d'obtenir une ligne marquée d'un astérisque `*`.
- Cet astérisque indique que le serveur NTP est **atteignable** et que la synchronisation est en cours.
- Attends quelques instants et relance la commande jusqu'à ce que le message **"Clock is synchronized"** apparaisse.

🧠 *Remarque pédagogique :*
Le routeur interroge périodiquement le serveur NTP pour ajuster son horloge.
Cette étape est essentielle avant de tester le Syslog, car des journaux non horodatés correctement seraient inutilisables en analyse d'incidents.

🕑 2️⃣ Vérification de l'horloge synchronisée

Une fois la synchronisation établie, vérifie l'heure actuelle du routeur :

```
R1# show clock
```

✅ **Exemple de résultat attendu :**

```
17:08:52.123 CEST Wed Sep 17 2025
```

Ce résultat montre que :

- L'heure est correcte et cohérente avec celle du serveur LOG-SRV,
- Le fuseau horaire (CEST, UTC, etc.) est pris en compte,
- Le protocole NTP fonctionne correctement.

💡 Points importants à retenir

- Le protocole **NTP** utilise le port **UDP 123**.
- La synchronisation peut prendre **jusqu'à 2 minutes** : patience requise !
- Sans NTP, les logs Syslog peuvent avoir des heures incohérentes → impossible d'analyser correctement les incidents.
- En entreprise, tous les équipements (routeurs, commutateurs, serveurs, pare-feux) doivent être synchronisés sur **la même source de temps**.

Partie 2 — Générer et vérifier les logs Syslog

Objectif :
Vérifier le bon fonctionnement du service **Syslog** en générant des événements sur le routeur **R1**, puis en s'assurant qu'ils sont bien envoyés et enregistrés sur le serveur **LOG-SRV**.

Cette étape valide la communication entre les équipements et prouve que les journaux sont centralisés et correctement horodatés grâce à la synchronisation NTP.

⚙️ 1️⃣ Génération d'événements sur le routeur

Maintenant que l'heure du routeur est juste, nous allons provoquer des événements réseau afin que des **logs** soient créés et transmis au serveur Syslog.
Le moyen le plus simple consiste à créer une **interface virtuelle (loopback)** et à la **désactiver / réactiver**.

Commandes à saisir sur R1 :

`R1# configure terminal` R1(config)# interface loopback 0 %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

`R1(config-if)# shutdown` %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down

`R1(config-if)# no shutdown` %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up`

🔍 **Observation :**
Chaque commande génère un message de log visible directement dans la **console du routeur**.
Ces messages signalent les changements d'état de l'interface et sont automatiquement envoyés au serveur Syslog configuré précédemment.

🖥️ 2️⃣ Vérification des logs sur le serveur Syslog

Étapes :

1. Aller sur le **serveur LOG-SRV**
2. Ouvrir l'onglet **Services** → **Syslog**
3. Observer la fenêtre de log en bas de l'écran

"Pasted image 20251029113248.png" ne peut être trouvé.

💡 **Résultat attendu :**
La fenêtre, auparavant vide, doit maintenant être remplie avec plusieurs lignes correspondant aux événements générés sur R1.

Exemple d'entrée typique :

```
Sep 17 17:09:01 192.168.1.1 %LINK-5-CHANGED: Interface Loopback0, changed state to up
```

🧠 **Analyse :**

- L'**horodatage précis** (grâce à NTP) apparaît au début de chaque ligne.
- L'adresse IP source `192.168.1.1` identifie le routeur R1.
- Le message indique l'événement survenu (changement d'état d'interface).

💡 Points importants à retenir

- Le **Syslog** centralise tous les journaux réseau pour simplifier la supervision et l'analyse.
- La **synchronisation NTP** garantit que tous les événements ont une heure exacte et comparable.
- La **création d'une interface loopback** est une méthode simple pour tester rapidement le bon fonctionnement du Syslog.
- En environnement professionnel, tous les routeurs, commutateurs et serveurs sont configurés pour envoyer leurs logs vers **un serveur Syslog unique**.