Implémentation de SNMP et Syslog

Topologie

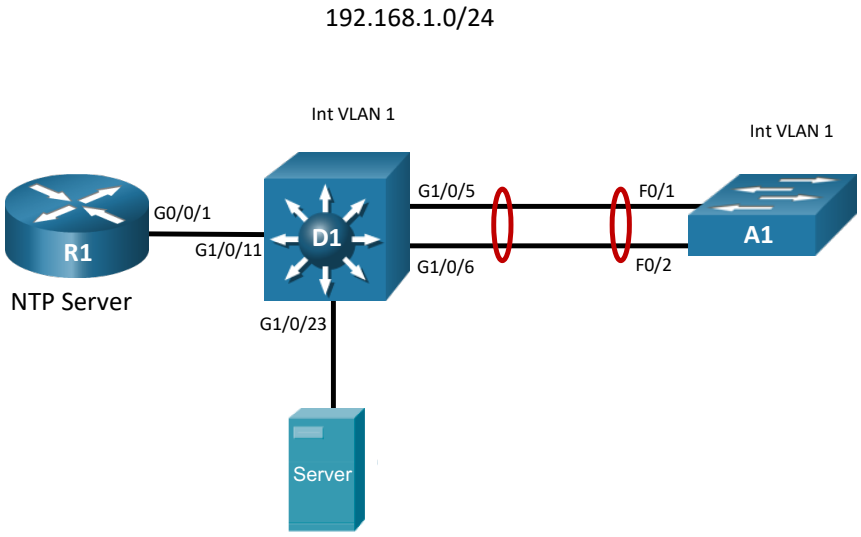

Table d'adressage

Device	Interface	IP Address
R1	G0/0/1	192.168.1.1/24
D1	VLAN 1	192.168.1.2/24
A1	VLAN 1	192.168.1.3/24
Server	NIC	192.168.1.50/24

Objectifs

- **Construire le réseau et configurer les paramètres de base ainsi que l'adressage des interfaces.**
- **Configurer et vérifier SNMP.**
- **Configurer et vérifier Syslog.**

Scenario

La surveillance réseau est essentielle pour les tâches de sécurité et de dépannage. À mesure que votre réseau se développe et évolue, une surveillance centralisée devient encore plus importante. **SNMP** est un protocole qui permet de surveiller à distance une large gamme de paramètres et de compteurs, d'être alerté en cas de changements et même d'effectuer des modifications de configuration à distance. **Syslog** est le protocole collecteur de journaux. Tous vos appareils devraient utiliser Syslog pour rapporter l'activité des appareils à un emplacement centralisé afin de permettre la corrélation et la conservation des enregistrements. Dans ce TP, vous configurerez ces deux protocoles extrêmement importants.

Resources à utiliser

- 1 Router (Cisco 4321)
- 1 Switch (Cisco 3650)
- 1 Switch (Cisco 2960)
- 1 Serveur (Server)

Part 1: Construire le réseau et configurer les paramètres de base des appareils et l'adressage des interfaces

Dans cette première partie, vous allez mettre en place la topologie réseau et configurer les paramètres de base ainsi que l'adressage des interfaces.

Étape 1 : Connectez le réseau comme indiqué dans la topologie

Reliez les appareils comme indiqué dans le schéma de la topologie et effectuez les connexions nécessaires

Étape 2 : configurer les paramètres de bases sur chaque appareil

Entrez en mode de configuration globale et appliquez les paramètres de base :

a. Configurez les adresses IP sur l'hôte Server comme indiqué dans la table d'adressage.

b. Activez NTP sur le Server et mettez l'horloge à UTC+1

c. configurer les trois équipements restants. Les configurations initiales pour chaque appareil sont fournies ci-dessous, étudiez et appliquez-les :

Router R1

```
hostname R1
no ip domain lookup
banner motd # R1, Implement SNMP and Syslog #
interface g0/0/1
 ip address 192.168.1.1 255.255.255.0
no shutdown
 exit
ntp server 192.168.1.50
end
```

Switch D1

```
hostname D1
no ip domain lookup
banner motd # D1, Implement SNMP and Syslog #
interface vlan 1
 ip address 192.168.1.2 255.255.255.0
no shutdown
 exit
ip default-gateway 192.168.1.50
interface g1/0/23
 switchport mode access
 no shutdown
 exit
interface g1/0/11
 switchport mode access
 no shutdown
 exit
interface range g1/0/5-6
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
 exit
interface range g1/0/1-4, g1/0/7-10, g1/0/12-22, g1/0/24, g1/1/1-4
 shutdown
 exit
ntp server 192.168.1.50
end
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, Implement SNMP and Syslog #
interface vlan 1
 ip address 192.168.1.3 255.255.255.0
no shutdown
 exit
ip default-gateway 192.168.1.1
interface range f0/1-2
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
 exit
interface range f0/3-24, g0/1-2
 shutdown
 exit
```

```
ntp server 192.168.1.50
end
```

d. Vérifiez que R1, D1 et A1 peuvent ping avec succès le Sever sur l'adresse 192.168.1.50

Configuration et vérification de SNMP

Le **Simple Network Management Protocol (SNMP)** est un protocole de la couche application qui facilite l'échange d'informations de gestion entre un agent et un serveur de gestion. SNMP permet aux administrateurs réseau de surveiller et de gérer les performances du réseau, d'identifier et de résoudre les problèmes, ainsi que de planifier l'évolution du réseau. Les stations de gestion SNMP peuvent demander (get) la valeur d'un identifiant d'objet spécifique (**OID**) à partir de la base d'informations de gestion (**MIB**) maintenue par les agents SNMP. Le gestionnaire peut également configurer (set) des valeurs spécifiques pour certaines variables dans un OID. En outre, l'agent peut envoyer des notifications (**traps** ou **informs**) lorsqu'un événement se produit ou qu'un seuil est atteint (un **inform** est une forme de trap qui doit être confirmé par le gestionnaire). Comme tout outil puissant, SNMP peut être dangereux s'il n'est pas utilisé correctement, et il est donc essentiel de sécuriser le protocole et ses usages.

Il existe trois versions de SNMP :

- **SNMPv1** et **SNMPv2** n'offrent ni authentification ni chiffrement.
- **SNMPv3** est considéré comme le plus sécurisé car il offre l'authentification et le chiffrement.

L'accès à SNMP peut également être limité en utilisant une liste de contrôle d'accès (**ACL**). **SNMPv3** est plus complexe à configurer, et son adoption n'est pas universelle. Dans ce TP, nous allons configurer **SNMPv2c**.

Step 1: Configuration des communautés SNMP.

SNMPv2c utilise une authentification basée sur une chaîne de communauté (**community string**). L'accès peut être davantage restreint en utilisant une liste de contrôle d'accès (**access list**). Créez une communauté en lecture seule nommée **EFREI** et **EFREI-RS** en lecture écriture. Configurez cela sur les trois appareils.

```
R1(config)# snmp-server community EFREI ro
R1(config)# snmp-server community EFREI-RS rw
```

Step 2: Requêtes SNMP

Sur la machine Server, lancer le navigateur MIB dans l'onglet Desktop. Dans le panel de gauche, dérouler la MIB et sélectionnez un OID (de votre choix), notez-le.

a. Lancer l'invite de commande sur le serveur et exécutez la commande **snmpget**, suivez la syntaxe proposer et faite une requête snmpget pour obtenir la valeur de l'OID que vous avez choisi sur le routeur R1.

b. Cherchez l'OID qui contient le nom du routeur, faite une requête **snmpset** pour changer le nom du routeur. Vérifier que ce dernier à bien changer sur le routeur.

c. Utiliser maintenant l'interface graphique du navigateur MIB pour exécuter des différents types de requêtes sur d'autres OID sur les trois équipements (utilisez les bouttons « advanced », « operation » et « go »).

Step 3: Analyse SNMP exchange.

Utilisez le mode simulation pour analyser ce qui se passe lors des opérations SNMP. A la fin de votre analyse **n'oubliez pas de quitter le mode simulation et revenir en mode Realtime.**

Part 2: Syslog

Pour de multiples raisons, la journalisation (logging) est une partie essentielle de votre plan de gestion de réseau. Les dispositifs journalisent sur trois installations générales : la console, le tampon de journalisation (logging buffer), et un serveur syslog, si configuré. Ces trois installations peuvent être contrôlées et configurées de manière à ce que le type de message de journal qu'elles enregistrent soit spécifique. La journalisation de la console permet simplement de visualiser les messages que l'appareil vous montre lorsqu'un événement se produit. Le tampon de journalisation collecte également ces mêmes informations. Ces deux éléments sont locaux à l'appareil. Ce que vous n'avez pas encore fait, c'est personnaliser ces installations, ni configurer et utiliser un serveur syslog centralisé, qui collecterait les messages de journal de chacun de vos appareils et les conserverait pour que vous puissiez examiner et corréler les événements entre différents appareils. Avant de configurer la journalisation, il est important que vos appareils soient synchronisés avec un serveur NTP, afin qu'ils soient tous sur la même heure. Cela rend possible le tri et la corrélation des événements.

Vous devez également avoir un plan pour séparer et gérer les messages de journal. Votre plan doit répondre aux questions suivantes : « Que faisons-nous de tous ces journaux ? » et « Quels messages vont où ? ». Les messages Syslog sont séparés en huit niveaux de sévérité différents, numérotés de 0 à 7. Les numéros les plus bas indiquent un message plus critique. Les niveaux de sévérité ont également des mots-clés :

Severity Level	Keyword	Meaning
0	emergencies	System is unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages

Step 1: buffered logging.

Le tampon de journalisation est configuré pour contenir 4096 octets dans un tampon circulaire et conserver les messages de journal au niveau de débogage et en dessous. 4096 octets ne sont pas suffisants pour un système occupé, il est donc nécessaire de modifier la taille du tampon de journalisation pour quelque chose de plus grand. Nous n'enverrons pas de messages de débogage au serveur syslog, donc le tampon est le seul endroit où ces messages sont stockés. Nous laisserons le niveau du tampon de journalisation sur débogage pour l'instant et réglerons la taille du tampon à 16384 octets. Configurez cela sur les trois dispositifs :

```
R1(config)# logging buffered 16384
```

Step 2: Configuration du service Syslog.

Ensuite, vous devez configurer l'adresse de l'hôte pour le serveur Syslog. Dans ce laboratoire, le serveur Syslog est 192.168.1.50. Configurez cela sur les trois appareils :

```
R1(config)# logging host 192.168.1.50
```

Step 3: Vérification de la configuration.

Vérifiez la configuration de l'appareil en exécutant la commande **show logging** à l'invite de commande privilégiée :

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: level debugging, 63 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 5 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level debugging, 68 message lines logged
        Logging to 192.168.1.50  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:

Log Buffer (16384 bytes):

*Jan 30 19:25:12.331: %SYS-5-LOG_CONFIG_CHANGE: Buffer logging: level debugging, xml
disabled, filtering disabled, size (16384)
*Jan 30 19:35:57.038: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.50 port
0 CLI Request Triggered
*Jan 30 19:35:58.039: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.50 port
514 started - CLI initiated
Jan 30 19:36:49.443: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Jan 30 19:37:58.857: %SYS-5-CONFIG_I: Configured from console by console
<output omitted>$$
```

Step 4: Analyse d'échange

Passer en mode simulation et analyser les échanges Syslog entre les équipements réseau et le serveur (en générant des logs, ex. changer l'état d'une interface) pour s'assurer que le service est bien configuré pour envoyer les messages log au serveur.

Step 5: Verification du service Syslog

a. Lancer le service Syslog sur le Server (onglet services), et vérifier que vous recevez bien les logs des trois équipements. Que remarquez-vous ?

b. Activer l'horodatage des logs sur les trois équipements avec la commande ci-dessous, vérifier.

```
R1(config)#service timestamps log datetime msec
```