Gestion de réseaux informatiques (GRX)

Chapitre 2: Syslog, Netflow (tiré de Cisco Academy)

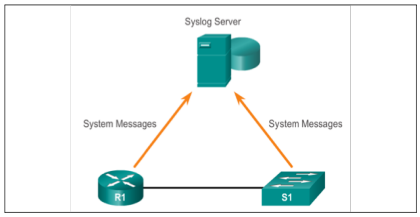
Stephan Robert

HAUTE ÉCOLE D'INGÉNIERIE ET DE GESTION DU CANTON DE VAUD
www.heig-vd.ch

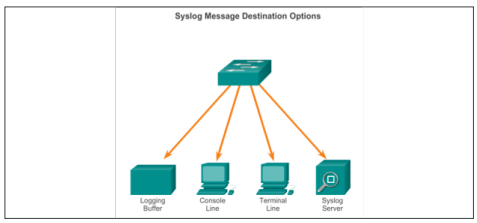
Objectifs

- Expliquer les opérations Syslog dans un réseau d'une PME
- Configurer syslog pour compiler les messages dans un environnement de PME
- Expliquer les opérations syslog dans un réseau de PME
- Décrire les opérations NetFlow dans un réseau de PME
- Configurer NetFlow sur un routeur pour exporter les données
- Examiner les données NetFlow pour déterminer les profiles de trafic

Introduction à Syslog



Opérations Syslog



4

Format des messages Syslog

Syslog Severity Level

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

For example, sample output on a Cisco switch for an EtherChannel link changing state to up is:

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

Here the facility is LINK and the severity level is 3, with a MNEMONIC of UPDOWN.

Syslog Message Format

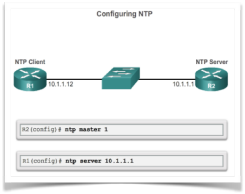
Field	Explanation
seq no	Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured.
timestamp	Date and time of the message or event, which appears only if the `service timestamps` global configuration command is configured.
facility	The facility to which the message refers.
severity	Single-digit code from 0 to 7 that is the severity of the message.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

5

Service de Timestamp

Opération Syslog

- Les messages de Log peuvent être « horodatés » ou « timestampés » et l'adresse de source des messages Syslog peut être fixée. Ça améliore le débogage en temps réel ainsi que la gestion du réseau
- La commande **`service timestamps log datetime`** est entrée dans le mode de configuration global et doit être entrée sur le dispositif.
- Dans ce chapitre il est sous-entendu que l'horloge a été synchronisée et que la commande **`service timestamps log datetime`** a été configurée sur tous les dispositifs

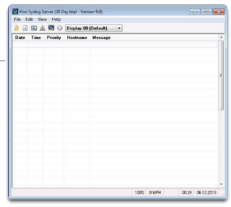


6

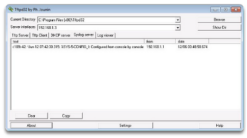
Serveur Syslog
Configuration de Syslog

- Le serveur Syslog fourni un interface « user-friendly » pour pouvoir visionner la sortie.
- Le serveur analyse la sortie et place les messages dans des colonnes prédéfinies pour faciliter l'interprétation. Si l'horodatage est configuré sur les périphériques réseau qui génèrent les messages syslog alors la date et l'heure de chaque message s'affiche sur la sortie du serveur syslog
- Les administrateurs réseau peuvent facilement naviguer parmi la grande quantité de données générée par le serveur syslog.

Syslog Server



Syslog Server



7

Log par défaut
Configuration de Syslog

```
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, 32 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 32 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 informational, 34 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):

*Jan  2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User
```

8

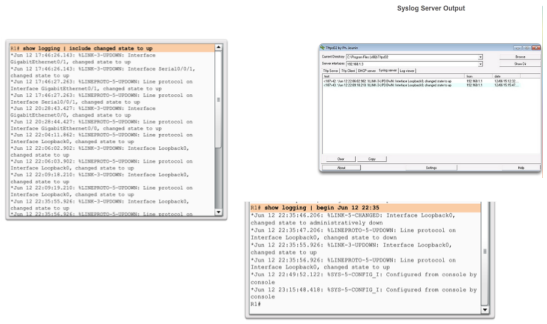
Commandes des routeurs et des switches pour les clients Syslog
Configuration de Syslog

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface gigabitEthernet 0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to
host 192.168.1.3 port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
R1(config-if)#
```

9

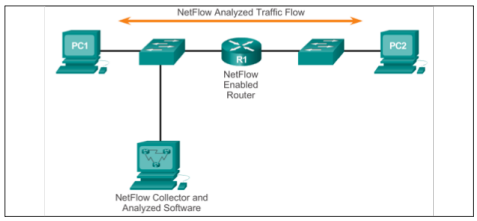
Vérification de Syslog

Configuration de Syslog



10

Introduction à Netflow



11

But de Netflow

Opérations avec Netflow

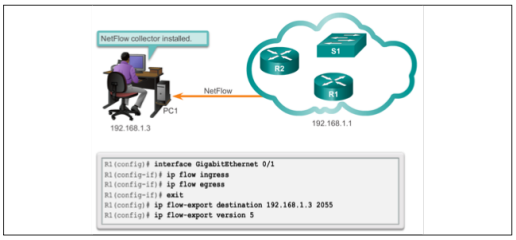
La plupart des organisations utilisent NetFlow avec pour objectif principal la collecte des données suivantes:

- Qui utilise les resources du réseau et dans quel but ?
- Facturation et comptabilité des utilisateurs en fonction de leur utilisation.
- Planification plus efficace en fonction des données mesurées. Allocation des resources pour satisfaire les exigence des clients.
- En utilisant l'information afin de mieux structurer et personnaliser l'ensemble des applications et des services pour répondre aux besoins des utilisateurs et les exigences en matière de service à la clientèle disponibles.

12

Tâches de configuration de Netflow

Configuration de Netflow



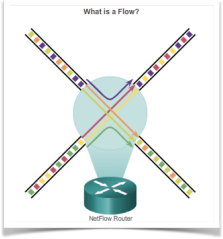
13

Flots Netflow

Opérations avec Netflow

La technologie NetFlow a vu plusieurs générations d'applications qui génèrent du trafic de plus en plus sophistiqué mais la version originale de Netflow distinguait les flots sur la base d'un ensemble de différents paramètres:

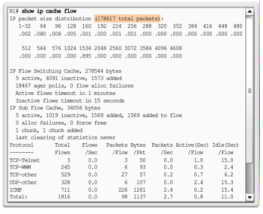
- Adresses IP de source et de destination
- Numéros de ports de source et de destination
- Type du protocole de niveau 3
- « Type of Service »
- Interface d'entrée logique

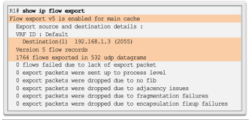


14

Vérifier Netflow

Examen du trafic

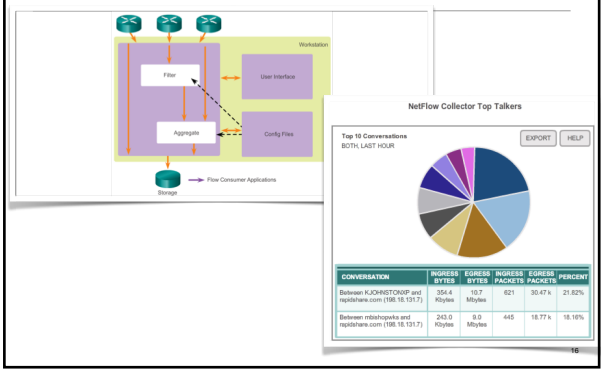




15

Fonctions du « Collector » de NetFlow

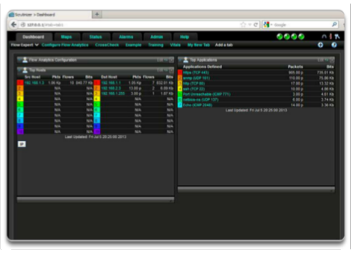
Examen du trafic



16

Analyse de NetFlow avec NetFlow Collector

Examen du trafic



17

Résumé

- **Syslog** et **NetFlow** sont des outils utiles pour l'administrateur réseau qui lui permettent de gérer, afficher, analyser une collection d'événements associés à des dispositifs réseau.
- **Syslog** est un outil rudimentaire pour collecter et afficher les messages qui apparaissent sur la console d'un routeur ou d'un switch.
- **NetFlow** (ou plus récemment: **Flexible NetFlow**) fournit un moyen de collecter des données opérationnelles de réseaux IP.
- **NetFlow** fourni des données qui permettent de gérer un réseau ainsi que sa sécurité, de planifier un réseau et d'analyser le trafic.
- Les collectors **NetFlow** fournissent des options sophistiquées d'analyse pour le flot de données.

18