Chapitre III

SUPERVISION RESEAU

Chapitre III

SUPERVISION RESEAU

III.1.Introduction

Les réseaux sont de partout à l'heure actuelle. Ils sont devenus indispensables au bon fonctionnement général de nombreuses entreprises et administrations. Tout problème ou panne peut avoir de lourdes conséquences aussi bien financières qu'organisationnelles. La supervision des réseaux est alors nécessaire et indispensable. Elle permet entre autre d'avoir une vue globale du fonctionnement et problèmes pouvant survenir sur un réseau mais aussi d'avoir des indicateurs sur la performance de son architecture. De nombreux logiciels qu'ils soient libres ou propriétaires existent sur le marché. La plupart s'appuie sur le protocole SNMP.

Dans une première partie nous allons faire une présentation de la supervision et tout ce qui touche au monitoring de réseau. Dans une seconde partie, nous verrons le fonctionnement du protocole le plus utilisé actuellement : le protocole SNMP.

III.2.Présentation

III.2.1 Définition de la supervision

En informatique, la supervision est une technique de suivi, qui permet de surveiller, analyser, rapporter et d'alerter les fonctionnements normaux et anormaux des systèmes informatiques.

Entre outre, La supervision informatique consiste à indiquer et/ou commander l'état d'un serveur, d'un équipement réseau ou d'un service software pour anticiper les plantages ou diagnostiquer rapidement une panne

III.2.2.Objectifs

Il est aujourd'hui de plus en plus difficile d'administrer un réseau. En effet le nombre d'équipements à gérer est souvent de plus en plus important : stations, serveurs, imprimantes… Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires.

Il faut pouvoir surveiller de manière continu l'état des systèmes d'information afin d'éviter un arrêt de production de trop longue durée. C'est là ou la supervision intervient. Elle doit permettre d'anticiper les problèmes et de faire remonter des informations sur l'état des équipements.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils indispensables.

III.2.3.Principe

Une grande majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années. Nous en faisons la description dans la deuxième partie.

La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information
- Visualiser l'architecture du système
- Analyser les problèmes
- Déclencher des alertes en cas de problèmes
- Effectuer des actions en fonction des alertes

La tache de l'administrateur est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée. Chaque outil doit aussi lui donner une vision globale du système d'information pour localiser les problèmes le plus rapidement possible.

III.3. Le protocole SNMP

III.3.1.Présentation

SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). C'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques. Ce protocole est donc utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau.

Chaque machine, que ce soit sous Windows ou sous Linux possède de nombreuses informations capitales pour l'administrateur réseaux. On retrouve des informations comme la quantité de RAM utilisé, l'utilisation du CPU, l'espace disque et encore bien d'autre indicateurs.

SNMP va permettre de remonter ces informations à l'administrateur de façon centralisé pour pouvoir réagir au plus vite aux pannes éventuelles.

III.3.2 .Fonctionnement

III.3.2.1 Les agents

Sur une machine à superviser, pour que SNMP envoie les informations que l'on souhaite il faut qu'un agent soit installé sur celle-ci. Cet agent écoute sur le port 161 et attend que le serveur lui envoie des requêtes pour lui répondre.

L'agent pourra aussi envoyer des alertes lui même si l'administrateur l'a configuré. Par exemple pour surveiller l'occupation CPU l'administrateur définira une valeur critique pour laquelle une alerte doit lui être émise.

Pour finir l'agent pourra aussi agir sur l'environnement local. C'est pourquoi ce protocole est critique car il peut servir a d'autres personnes mal intentionnées pour prendre le contrôle a distance de certains équipements sur le réseau.

III.3.2.2 Les systèmes de management de réseaux

Généralement, l'administrateur possède un outil permettant de centraliser ce que lui retournent ses agents. Et c'est donc cet outil qui va interroger les équipements du réseau. Il va donc pouvoir gérer un réseau entier grâce à cela.

III.3.2.3 La MIB

- • Présentation

Pour que SNMP fonctionne, il est nécessaire qu'un protocole d'échange soit définit. Il y a aussi une standardisation des informations que ce protocole peut transporter. C'est un protocole Internet, il doit être utilisable sur des plates-formes hétérogènes (matériel comme système d'exploitation).

C'est pour cette raison que l'on parlera de MIB (Management Information Base).En effet, la MIB est une base de données des informations de gestion maintenue par l'agent. C'est cette base à laquelle on va demander les informations.

- • Structure de la MIB

La structure de la MIB est hiérarchique : les informations sont regroupées en arbre. Chaque information a un OID (Object identifier), une suite de chiffres séparés par des points, qui l'identifie de façon unique et un nom, indiqué dans le document qui décrit la MIB.

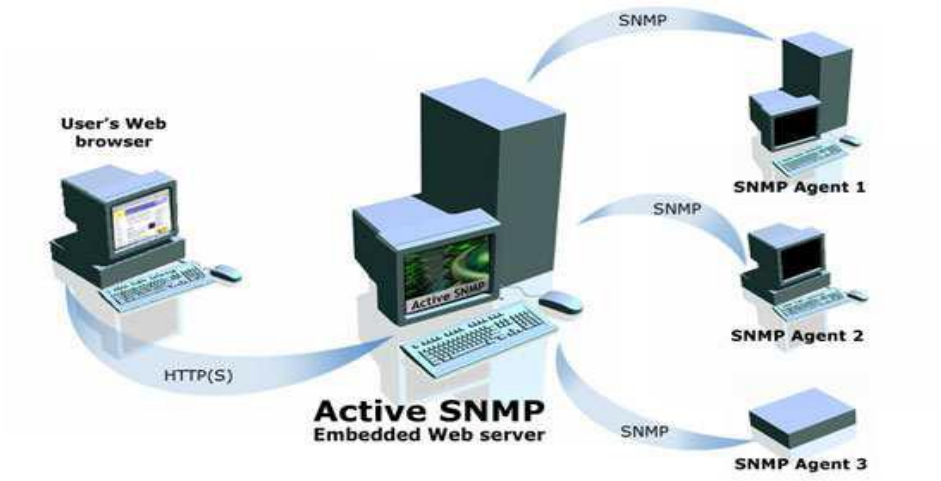

Figure III.1: Eléments de base du protocole SNMP

III.3.2.4.Les commandes SNMP

Il existe 4 types de requêtes SNMP :

- get-request : Le Manager SNMP demande une information à un agent SNMP
- get-next-request : Le Manager SNMP demande l'information suivante à l'agent SNMP

- set-request : Le Manager SNMP met à jour une information sur un agent SNMP
- trap : L'agent SNMP envoie une alerte au Manager

Les alertes sont transmises lorsqu'un événement non attendu se produit sur l'agent. Ce dernier informe le manager via une « trap ». Plusieurs types d'alertes sont alors possibles : ColdStart, WarmStart, LinkDown, LinkUp, AuthentificationFailure.

Pour chaque envoi de message, une réponse est retournée à l'exception de la commande « trap ». Les réponses sont du type suivant :

- get-response : L'information a bien été transmise.
- NoSuchObject : Aucune variable n'a été trouvée.
- NoAccess : Les droits d'accès ne sont pas bons.
- NoWritable : La variable ne peut être écrite.

III.3.2.5 Echange de message

Voici un schéma récapitulant les échanges pouvant être effectués entre un agent et le manager :

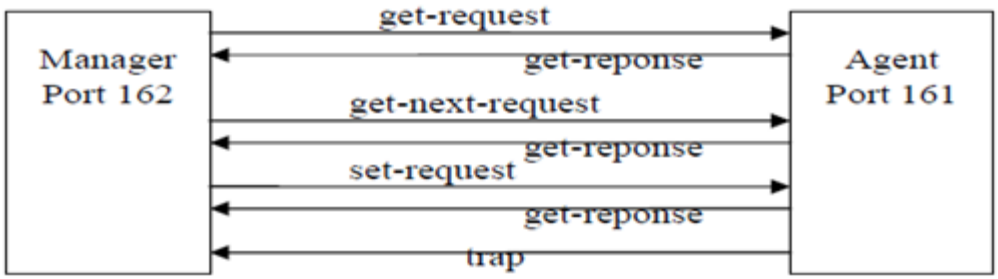

Figure III.2: Exemple d'échange SNMP

Le protocole SNMP est principalement utilisé avec UDP/IP. (Il peut aussi utiliser TCP). L'utilisation d'UDP permet un échange de message plus rapide que l'utilisation de TCP. L'inconvénient est qu'il est possible de perdre des trames lors de l'échange de messages (mode non connecté). Les ports UDP sont donc le 162 pour le manager et le 161 pour les agents.

III.3.3. SNMP en pratique

Concrètement, dans le cadre d'un réseau, SNMP est utilisé: pour administrer les équipements et pour surveiller le comportement des équipements Une requête SNMP est un datagramme UDP habituellement à destination du port 161. Les schémas de sécurité dépendent des versions de SNMP (v1, v2 ou v3). Dans les versions 1 et 2, une requête SNMP contient un nom appelé communauté, utilisé comme un mot de passe. Il y a un nom de communauté différent pour obtenir les droits en lecture et pour obtenir les droits en écriture.

Dans bien des cas, les colossales lacunes de sécurité que comportent les versions 1 et 2 de SNMP limitent l'utilisation de SNMP à la lecture des informations car la communauté circule sans chiffrement avec ces deux protocoles. Un grand nombre de logiciels libres et propriétaires utilisent SNMP pour interroger régulièrement les équipements et produire des graphes rendant compte de l'évolution des réseaux ou des systèmes informatiques (MRTG, Cacti, Nagios, Zabbix...)

III.4. Conclusion

La supervision est devenue indispensable dans tout système d'information. Elle est à la base du bon fonctionnement d'une architecture réseau et permet de réagir rapidement en cas de problèmes ou pannes. Elle se base à l'heure actuelle principalement sur le protocole SNMP qui depuis de nombreuses années a quand même du mal à évoluer. En effet, de nombreux logiciels sont encore basés sur la version 1 du protocole qui commence un peu à vieillir et qui n'est pas du tout sécurisé. En effet la version 2, apportant notamment la sécurité n'a été qu'une phase de transition vers la v3 qui est encore très peu utilisée.