

Renforcement des compétences des ressources du NOC

OUTILS DE SUPERVISION ET DE GESTION DES RÉSEAUX

Informations générales sur le document et versioning

Titre du document	Fondamentaux des réseaux, outils de supervision et de gestion des réseaux	
Version	1.0	
Auteurs	Steve FOTSO, Responsable NOC Edwige LONGMENE, Ing. DARS	
Date de publication	Juin 2024	
Amélioration 1 (V1.1)	Date: Juin 2024	Auteur: Steve FOTSO
Amélioration 1(V1.2)	Date:	Auteur:
Amélioration 1(V1.3)	Date:	Auteur:
Amélioration 1(V1.4)	Date:	Auteur:
Amélioration 1(V1.5)	Date:	Auteur:

Plan de la formation:

MODULE : Outils de gestion réseau et services

- Outils de diagnostics réseaux
- Objectif de la supervision réseau
- Types de supervision
- Les outils de monitoring de Matrix Télécoms S.A (Solar Wing, PRTG, CACTI, Uptime Robot)

Définition et objectif de la supervision réseau

- La supervision réseau **consiste à collecter, analyser et surveiller en continu** les informations de performance et de disponibilité de l'ensemble des équipements et services du réseau.

Ses principaux objectifs sont :

- Déetecter et résoudre les défaillances avant impact utilisateur
- Optimiser les ressources et capacités
- Garantir les niveaux de service (SLA)
- Planifier les extensions et modernisations



Définition et objectif de la supervision réseau

- Comprendre les concepts de monitoring est essentiel pour garantir les performances, la disponibilité et la sécurité d'une infrastructure informatique. Voici les principaux concepts liés au monitoring :

Principaux concepts liés au monitoring :

1/ Collecte de métriques

- Collecter des données clés sur les performances des systèmes (CPU, mémoire, disque, bande passante réseau, etc.)
- Surveiller les journaux d'événements et les logs applicatifs pour détecter les erreurs et les problèmes.

2/ Surveillance active et passive

- Surveillance active : tester régulièrement la disponibilité des services (ping, requêtes HTTP, etc.)
- Surveillance passive : analyser les flux de trafic réseau et collecter les métriques envoyées par les équipements.



Définition et objectif de la supervision réseau

Outils de gestion réseau et services



4. Cartographie des dépendances

- Comprendre les relations entre les différents composants d'une infrastructure (applications, serveurs, réseaux, etc.)
- Pouvoir visualiser l'impact d'un problème sur l'ensemble de l'infrastructure.

5. Corrélation d'événements

- Analyser et corrélérer les différents événements pour identifier la cause racine d'un problème.
- Éviter les alertes redondantes et faciliter le diagnostic.

6. Rapports et analyses historiques

- Générer des rapports détaillés sur les performances et la disponibilité des systèmes.
- Analyser les tendances et les modèles grâce aux données historiques collectées.

8. Supervision centralisée

- Regrouper la surveillance de tous les systèmes dans une console centralisée
- Faciliter la gestion et la visualisation de l'ensemble de l'infrastructure.

Types de supervision réseau

On distingue différents types de supervision selon l'aspect du réseau surveillé :

- **Supervision de disponibilité** : Uptime des équipements
- **Supervision de performance** : Bande passante, charge, latence
- **Supervision du trafic** : Volumes, pics, analyse des flux
- **Supervision de gigue** : Fluctuations de latence
- **Supervision de configuration** : Conformité des équipements
- **Supervision de sécurité** : Attaques, accès non autorisés

Outils de gestion réseau et services

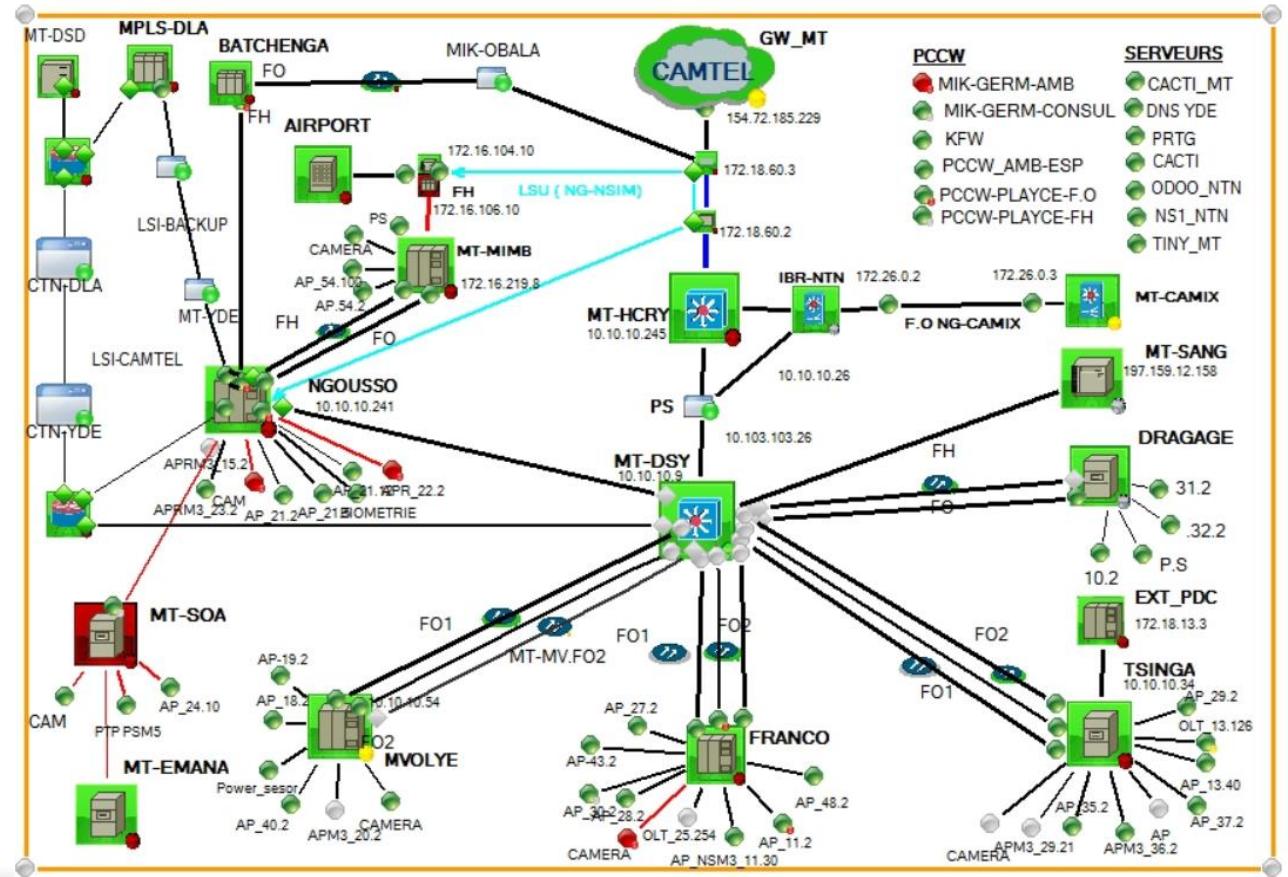


Il existe de nombreuses solutions de supervision réseau, parmi lesquelles :

- **SolarWinds** : Outil très complet couvrant disponibilité, performance, configuration, logs, troubleshooting.
- **PRTG** : Focalisé sur la supervision d'infrastructure et d'applications, avec une utilisation simplifiée.
- **Cacti** : Solution orientée graphiques de performance et disponibilité.
- **Uptime Robot** : Solution orientée graphiques de performance et disponibilité.

Présentation de SolarWinds

SolarWinds Network Performance Monitor est un outil de surveillance, de gestion et de dépannage de réseaux informatiques. C'est une solution logicielle complète qui permet de surveiller en temps réel les performances et la disponibilité des équipements réseau de notre backbone:



Présentation de SolarWinds

Outils de gestion réseau et services



Fonctionnalités de SolarWinds NPM utilisées:

1. Surveillance en temps réel de l'état des équipements réseau

1. Détection automatique des nouveaux équipements
2. Collecte de métriques de performance (bande passante, trafic, latence, etc.)
3. Génération d'alertes en cas de problèmes

2. Cartographie et visualisation du réseau

1. Vue en temps réel de l'état et de la connectivité des équipements
3. Dépannage et résolution des problèmes Outils de diagnostic avancés (traceroute, ping, capture de paquets)
4. Analyses de trafic et de performances historiques



Visite guidée de la plateforme solarwinds

Présentation de PRTG



Visite guidée de la plateforme

Outils de
gestion réseau
et services



Présentation de CACTI : Création de graph

Cacti est un logiciel libre de mesure de performances d'un réseau sur la puissance de stockage de données de RRDTool. Il ne fait pas de supervision en tant que tel et ne fait pas de corrélation d'incidents ni d'alerte en cas d'incident.

Dans notre réseau, il permet de ressortir les graphes de consommation des différents clients et de quelques liaisons importantes tels que les sorties

Pour la création des graphs, il suffit de se rendre à la **console** d'administration une fois logger à la plateforme et ensuite sur l'onglet **Devices (1) (2)**

Ensuite cliquez sur **Add** pour ajouter un équipement (3)

Puis remplir les différents champs relatifs à l'équipement et cliquer sur créer (create)

Champs	Descriptions
Description	Nom
Hostname	IP
SNMP Version	Version SNMP utilisé sur l'équipement

Enfin ajouter le type de données à extraire : dans notre cas c'est le trafic sur les interfaces (5)

1

2

3

5

Présentation de CACTI : Création de graph

Une fois l'équipement ajouté il est temps de créer le graph extrait à partir des interfaces, Pour cela cliqué sur **Create Graphs for this Host (6)**

Ensute sélectionné l'interface sur lequel créer le graph et le type de graph (7) (8)

- * **Create Graphs for this Host**
- * **Data Source List**
- * **Graph List**

6

7

8

Data Query [SNMP - Interface Statistics]					
Index	Status	Description	Type	Speed	Hardware Address
1	Up	lo	softwareLoopback(24)	0	
2	Up	eth0	ethernetCsmacd(6)	100000000	24:A4:3C:6F:09:6E
3	Down	eth1	ethernetCsmacd(6)	0	26:A4:3C:6F:09:6E
4	Up	wifi0	ethernetCsmacd(6)	0	24:A4:3C:6E:09:6E
5	Up	ath0	ethernetCsmacd(6)	130000000	24:A4:3C:6E:09:6E
6	Up	br0	ethernetCsmacd(6)	0	24:A4:3C:6E:09:6E

Select a graph type

Outils de gestion réseau et services

Présentation de Uptime Robot

Outils de
gestion réseau
et services



Visite guidée de la plateforme

Ajout des nœuds/Clients

L'ajout des éléments à superviser (routeurs, serveurs, applications...) se fait généralement par :

- Découverte automatique du réseau
- Import de plages d'adresses IP ou de listes d'équipements
- Ajout manuel au cas par cas

Outils de gestion réseau et services



Cas pratique : Solarwinds

1

Entrer l'adresse IP de l'équipement à montrer

2

Définir la méthode de collecte :
ICMP pour montrer uniquement la disponibilité
SNMP pour les équipements qui supportent le protocole

3

Tester le SNMP pour les équipements qui supportent afin
De valider

4

Supervision des machines / serveurs

Define Node

Specify the node you want to add by completing the fields below. Are you adding a large number of nodes? Try the [Network Discovery](#).

Polling Hostname or IP Address: IPv4 and IPv6 formats are both valid

Dynamic IP Address (DHCP or BOOTP)

Polling Method: [Help me choose a polling method](#)

External Node: No Status

No data is collected for this node. Useful for monitoring a hosted application or other element on the node but not the node itself.

Status Only: ICMP

Limited data (status, response, packet loss) is collected using ICMP (ping). Useful for devices which do not support SNMP or WMI.

Most Devices: SNMP and ICMP

Standard polling method for network devices such as switches and routers, as well as Linux and Unix servers.

SNMP Version:

SNMPv2c is used, by default, when SNMPv3 is neither required nor supported.

SNMP Port:

Allow 64 bit counters

Community String:

Press down arrow to view all

Read/Write Community String:

TEST

Windows Servers: WMI and ICMP

Recommended agentless polling method for Windows servers.

Windows & Linux Servers: Agent

Optional agent useful for monitoring Windows & Linux hosts in remote environments, such as the cloud. Credentials are needed only for installing the agent. The agent does not need to be installed on the server already. [What is an agent?](#)

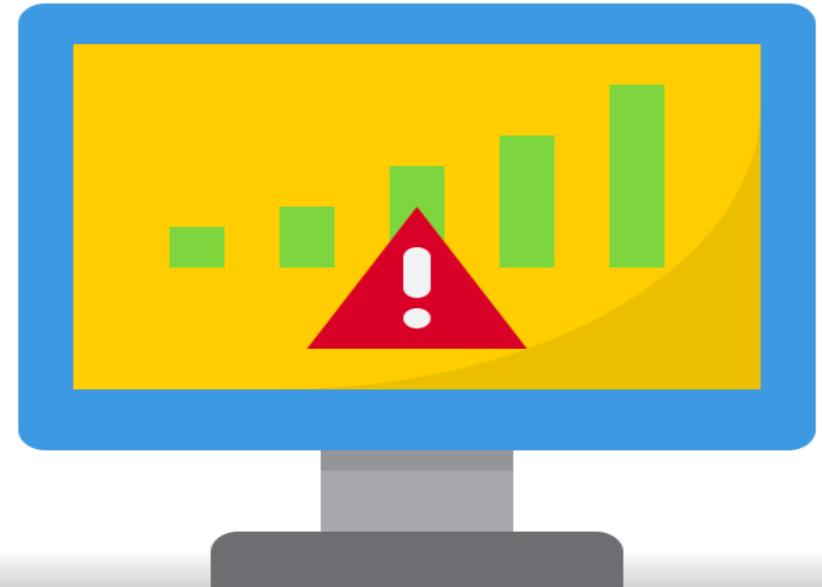
4

Interprétation des alertes

Les solutions de monitoring génèrent des alertes en cas de dépassement des seuils configurés. Les principales sont :

- Indisponibilité d'un équipement
- Dépassement de seuils de charge, bande passante, etc.
- Erreurs dans les logs systèmes

Il faut pouvoir hiérarchiser, filtrer et acheminer correctement ces alertes.



Cas pratique 1 : Solarwinds / PRTG

Interprétation des logs

Les journaux d'événements (syslogs) concentrés par la supervision permettent de détecter et d'analyser des problèmes.

Par exemple :

- Erreurs matérielles ou logicielles
- Pannes de modules
- Attaques de sécurité
- Changements de configuration

Il faut savoir extraire les informations pertinentes de ces logs.



Cas pratique : Solarwinds / PRTG