

Nama : Muhamad Yusup

NIM : 09011281419061

## **Nagios Sebagai *Network Monitoring Software***

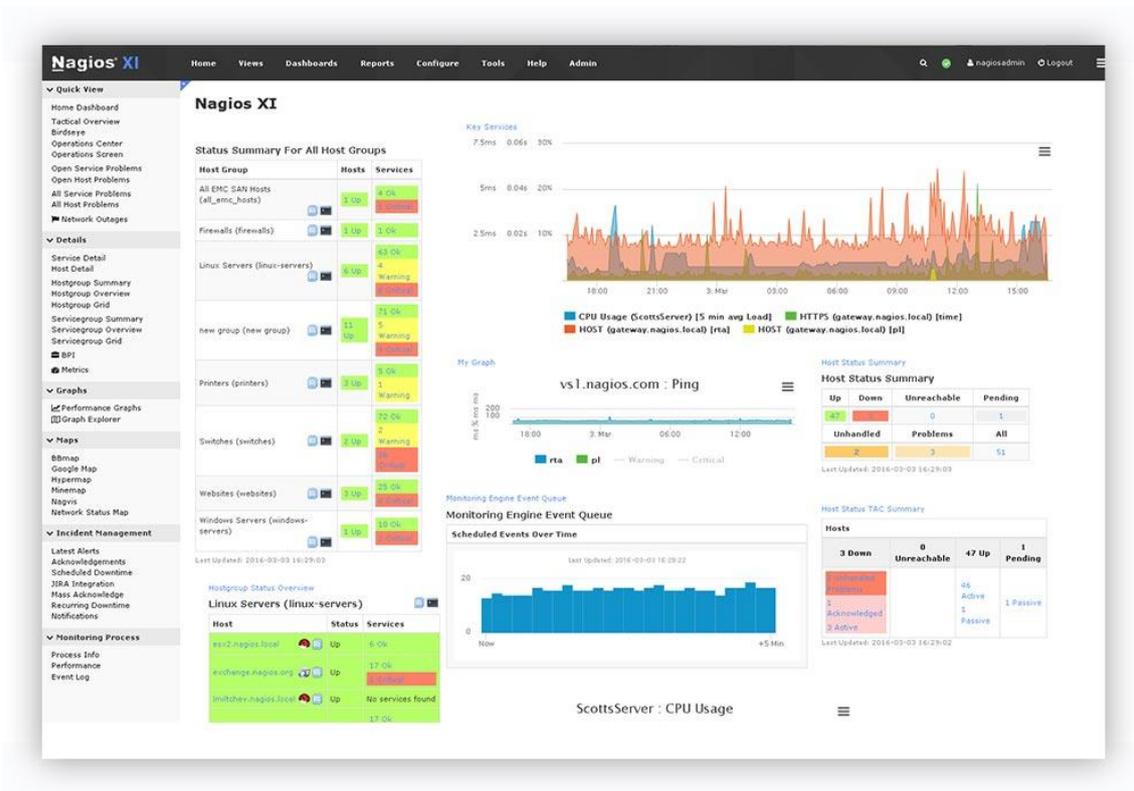
### **1. Pendahuluan**

Nagios adalah NMS *open source* yang dirancang khusus untuk memonitor *host/managed device* dan layanan jaringan serta untuk menginformasikan event-event yang terjadi pada jaringan, misalnya koneksi jaringan putus kepada administrator jaringan melalui beberapa cara, yaitu melalui *e-mail*, *instant message*, SMS, dan antarmuka *web*. Nagios juga mendukung *security management* yang terdefinisi pada standard FCAPS. Dalam definisi lain juga dikatakan bahwa Nagios merupakan suatu host dan service yang di design untuk memonitoring keadaan suatu jaringan atau bisa memonitoring masalah-masalah pada suatu host tertentu yang ingin kita monitoring. Nagios mengawasi host-host dan servis yang telah ditetapkan, memberi peringatan jika keadaan memburuk, dan memberi tahu kapan keadaan tersebut membaik.

Nagios telah terbukti populer di kalangan usaha kecil. Pengguna lainnya termasuk penyedia layanan Internet (ISPs), lembaga pendidikan, instansi pemerintah, lembaga perawatan kesehatan, perusahaan manufaktur, dan lembaga keuangan. Sebelumnya disebut NetSaint, nagios dikembangkan oleh Ethan Gelstad dan disempurnakan oleh banyak kontributor.

Untuk melakukan fungsi manajemennya, Nagios dilengkapi dengan sekumpulan *plugin* yang dapat memonitor status layanan lokal dan *remote*. *Plugin* adalah program kecil/ *script* dalam berbagai bahasa pemrograman yang digunakan untuk mengecek suatu layanan, misalnya *free space harddisk* dari host atau *managed device*. *Plugin* dapat dijalankan secara lokal maupun *remote* tergantung layanan yang akan dimonitor. *Plugin-plugin* tersebut melakukan *polling* terhadap layanan lokal atau *remote* secara berkala dengan interval waktu yang telah ditentukan dan mengirimkan status atau hasil monitoring tersebut kepada server Nagios.

Selain itu, terdapat juga plugin yang dirancang untuk mendeteksi *event-event* yang terjadi pada sebuah jaringan. Ketika *plugin* mengembalikan pesan peringatan atau *error* pada server Nagios, maka server Nagios tersebut akan mengirimkan notifikasi pada administrator jaringan melalui *e-mail* atau *sms* atau *instans message*. Berikut tampilan antarmuka dari *network monitoring software open source* Nagios.



Gambar 1 Antamuka web NMS Nagios

Nagios sendiri terdiri dari tiga bagian, yaitu :

- Scheduler* sebagai server Nagios. Pada interval berkala, *scheduler* mengecek *plugin* dan berdasarkan hasil pengecekan, server Nagios akan melakukan aksi.
- GUI (*Graphical User Interface*) sebagai antarmuka nagios berbasis web.
- Plugin* yang dapat dikonfigurasi oleh administrator jaringan. *Plugin* ini akan mengecek status layanan dan mengirimkan hasilnya pada server Nagios.

Secara keseluruhan, Nagios memiliki beberapa keistimewaan diantaranya :

- a. Memonitoring service jaringan (SMTP, POP3, HTTP, NNTP, PING, dan sebagainya).
- b. Service cek yang parallel.
- c. Web interface yang informatif untuk melihat status network (urutan masalah dan pemberitahuan, log file, dan sebagainya).
- d. Memonitoring sumber-sumber host (load prosesor, penggunaan disk, dan sebagainya).
- e. Desain plugin yang sederhana, yang memungkinkan pengguna lebih mudah menggunakan pemeriksaan terhadap service.
- f. Kemampuan untuk mendefinisikan kejadian yang ditangani selama service atau host berlangsung untuk mempermudah pemecahan masalah
- g. Perputaran file log yang otomatis.
- h. Pemberitahuan ketika terjadi masalah pada servis atau host dan mendapatkan pemecahannya ( lewat email, atau metode user-defined).

## 2. Fitur-fitur dalam Nagios

Nagios memiliki berbagai fitur yang mendukungnya dalam melakukan monitoring jaringan, diantaranya adalah sebagai berikut :

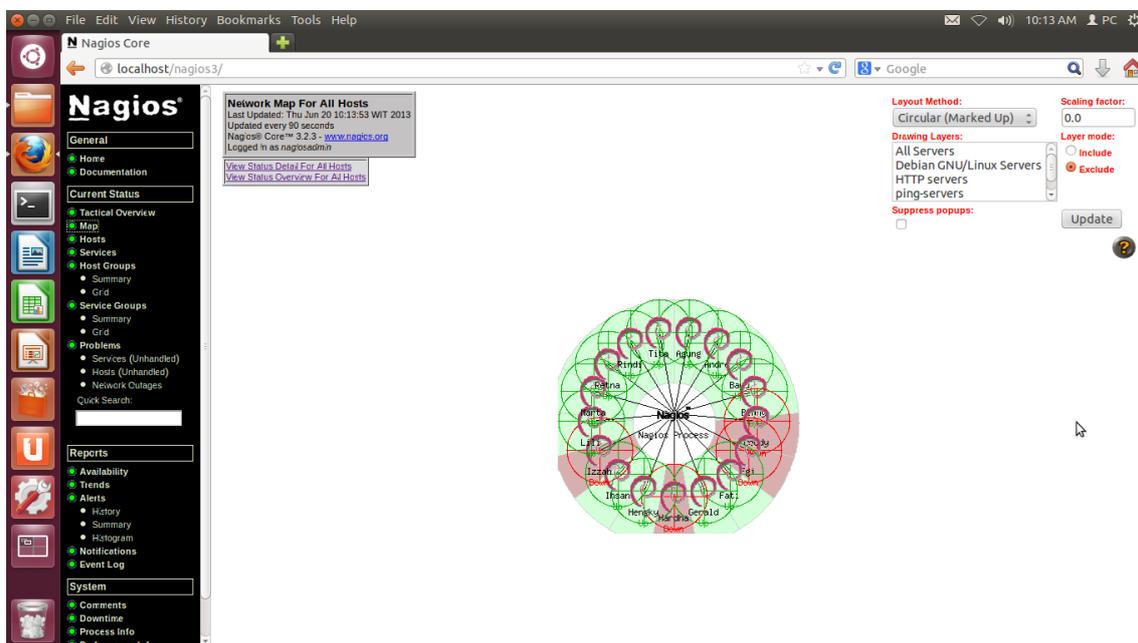
No.	Fitur	Fungsi Manajemen yang berkorelasi	Kategori FCAPS
1.	Memonitor layanan jaringan (SMTP, POP3, HTTP, PING, dll)	<i>Performance data collection</i>	<i>Performance Management</i>
2.	Memonitor sumber daya host ( <i>Proessor load, disk, dan memory usage, running process, file log, dll</i> )	<i>Performance data collection</i>	<i>Performance Management</i>
3.	Mendeteksi dan membedakan antara host yang <i>down</i> dan host yang <i>unreachable</i>	<i>Fault detection</i>	<i>Fault Management</i>
4.	Kemampuan mendefinisikan event handler untuk penyelesaian problem yang bersifat proaktif	<i>Fault correction</i>	<i>Fault Management</i>
5.	Penjadwalan <i>downtime</i>	<i>Network recovery</i>	<i>Fault Management</i>

6.	Mendeteksi dan melaporkan anomaly dan serangan pada sistem	<i>Security alarm and event reporting</i>	<i>Security Management</i>
----	--	---	----------------------------

Lebih lengkapnya, berikut penjelasan detail fitur-fitur yang ada dalam Nagios sebagai referensi tambahan dalam tugas ini :

a. Status Map

Yang dapat kita lihat pertama kali setelah melakukan penginstalan Nagios adalah status map jaringan yang kita miliki. Dari status map kita mengetahui host yang mana yang sudah UP ataupun yang masih PENDING bahkan DOWN.



Gambar 2 Status Map

b. Hosts

Host merupakan salah satu object sentral dalam monitoring logic. Sifat – sifat penting dari host tersebut adalah :

- Host biasanya merupakan perangkat fisik dalam suatu jaringan seperti router, switch, printer, PC, dan sebagainya.
- Host mempunyai alamat sendiri seperti IP Address atau MAC Address.
- Host memiliki satu atau lebih layanan yang berhubungan dengannya.

Dalam fitur host, kita dapat melihat status detail para host dalam satu grup yang telah dikonfigurasi pada hostgroupsnya. Ada beberapa fitur pada Host Status Details for All Groups, seperti :

- STATUS

Status disini berfungsi untuk mengetahui apakah host – host tersebut dalam keadaan UP (aktif) atau DOWN.

- LAST CHECK

Berfungsi untuk mengetahui kapan terakhir kali dilakukan pemeriksaan host – host tersebut.

- DURATION CHECK

Berapa lama durasi pengecekan yang dilakukan.

- STATUS INFORMATION

Status information berfungsi sebagai keterangan dari suatu host tersebut. Apakah ia UP (aktif) atau DOWN. Apabila UP, keterangan yang ditampilkannya adalah berapakah packet loss nya dan berapa lama RTA (Real Time Analysis) nya. Sedangkan apabila DOWN, keterangan pada Status Information dapat bermacam – macam.

c. Hostgroups

Hostgroup adalah grup dari satu atau lebih host. Hostgroup memudahkan kita untuk melihat status details dari host – host yang bersangkutan.

d. Service

Services juga merupakan salah satu object sentral dalam monitoring logic. Services berhubungan dengan host, karena :

- Services adalah atribut dari host (CPU load, disk usage, uptime, etc).
- Services ditetapkan oleh host, seperti DNS Record, dll.

Ada bermacam – macam service yang bisa digunakan untuk host, tetapi pada konfigurasi yang saya lakukan, terdapat tujuh services yaitu Current Load, Current Users, Disk Space, HTTP, PING, SSH dan Total Processes. Ketujuh service ini lah yang akan dimonitoring oleh host dalam suatu jaringan.

e. Problems

Dari fitur problem ini, terdapat beberapa sub menu yang bisa kita lihat. Ada Services (Unhandled), Hosts (Unhandled), dan Network Outages. Dari fitur submenu pada Problem ini kita dapat melihat apa - apa saja yang menjadi masalah pada konfigurasi monitoring host kita

f. Report.

Report disini berfungsi untuk mengetahui gangguan yang terjadi pada tiap – tiap services hostgroupnya. Sehingga kita dapat mengetahui persen dari Time Up, Time Down, Time Unreachable, dan Time Undetermined nya.