

IMPLEMENTASI NETWORK MONITORING SYSTEM MENGGUNAKAN NAGIOS DAN NAGVIS PADA PT. PELNI (PERSERO)

Rizky Fauzi¹, Desmulyati²

Program Studi Teknik Informatika^{1,2}

STMIK Nusa Mandiri Jakarta^{1,2}

rizkyf12180550@nusamandiri.ac.id¹, desmulyati.dmy@nusamandiri.ac.id²

Abstrak

Perkembangan teknologi dan jaringan komputer pada saat ini sangatlah pesat, sudah banyak perusahaan dan instansi pemerintah yang memanfaatkan jaringan sebagai salah satu sistem komunikasi antar satu dengan yang lainnya. Seperti pada PT. PELNI (Persero) perusahaan yang bergerak dibidang jasa transportasi laut, memiliki kantor cabang yang tersebar diseluruh Indonesia dan saling terhubung ke data center dengan memanfaatkan koneksi jaringan VPN. Dalam melakukan penelitian ini penulis melakukan observasi dengan melakukan pengamatan langsung ke lapangan dan metode wawancara pada staf ahli yang ada di Divisi Teknologi Informasi. Selain itu juga dilakukan studi kepustakaan untuk menunjang penelitian sehingga dapat menjadi acuan atau dasar dalam penyusunan laporan penelitian ini. Dari penelitian yang dilakukan, diperoleh bahwa pada perusahaan ini tidak memiliki *Network Monitoring System* sehingga apabila terjadi masalah pada jaringan ataupun server harus melakukan pengecekan secara manual. Dengan menggunakan Nagios dan Nagvis sebagai dashboard pada PT. PELNI (Persero) ini untuk memudahkan administrator dalam memantau seluruh jaringan dan perangkat server yang ada di perusahaan. Hasil pengujian jaringan akhir menggunakan aplikasi Nagios sebagai *network monitoring* dan Nagvis sebagai *dashboard* menambahkan *host* untuk dapat dimonitoring melalui aplikasi Nagios, terlihat tampilan status (*Up*) apabila *host* dalam keadaan aktif dan menampilkan status (*Down*) apabila *host* dalam keadaan tidak aktif.

Kata Kunci: Jaringan Komputer, VPN, *Network Monitoring System*, Nagios, Nagvis

I. PENDAHULUAN

Perkembangan teknologi dan jaringan komputer pada saat ini sangatlah pesat, sudah banyak perusahaan dan instansi pemerintah yang memanfaatkan jaringan sebagai salah satu sistem komunikasi antar satu dengan yang lainnya. Seiring dengan berjalannya waktu, lingkungan perusahaan menjadi sangat luas cakupannya hingga masuk menjadi kategori *Wide Area Network (WAN)*. Pada saat ini melakukan pemantauan terhadap jaringan menjadi sangat sulit apabila jaringan sudah menjadi sangat luas. Masalah yang sering terjadi dalam lembaga pemerintah salah satunya adalah kerusakan elemen jaringan seperti *router*, *modem* dan sebagainya. Perkembangan jaringan pada perusahaan ini memicu dibutuhkannya suatu sistem yang bisa memantau seluruh jaringan komputer dan perangkatnya. Solusi yang dapat digunakan adalah dengan menggunakan *Network Monitoring Sistem*.

Diperlukan sebuah fasilitas pendukung yaitu *network monitoring system* agar *network administrator* dapat memonitor suatu perangkat ataupun *service* pada suatu jaringan meskipun tidak di depan komputer secara langsung [1]

Banyaknya perangkat jaringan yang ada di seluruh kantor cabang dan perangkat *server* yang ada di *data center* kantor pusat akan menyulitkan *administrator* untuk memonitor satu per satu perangkat yang terkoneksi ke jaringan.

Dengan penggunaan nagios sebagai aplikasi *monitoring* dan nagvis sebagai *dashboard* dapat menjadi sebuah alternatif yang baik dalam melakukan pemantauan jaringan dan *server*. Nagios sendiri dapat dikonfigurasi sesuai dengan kebutuhan, seperti pemanfaatan *plugin* nagvis agar terintegrasi dengan nagios yang bisa digunakan sebagai *dashboard* untuk menampilkan seluruh *host* yang di monitor dan akan memberikan *alert* secara langsung. Nagios merupakan aplikasi yang bersifat *open source* sehingga dapat di kustomisasi sesuai kebutuhan dan tidak akan memberatkan dari segi biaya lisensi.

II. LITERATUR

Dengan berkembangnya teknologi komputer dan komunikasi suatu model komputer tunggal yang melayani seluruh tugas-tugas komputasi suatu organisasi kini telah diganti dengan sekumpulan

komputer yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, sistem seperti ini disebut jaringan komputer (*Computer Network*). Jaringan komputer adalah interkoneksi beberapa buah komputer *autonomous* (independen) yang dapat saling berbagi informasi dan sumber daya [2].

1. Jenis-jenis Jaringan Komputer

- a) *Local Area Network* (LAN)
Local Area Network adalah jaringan yang dibuat pada area terbatas (tertutup). Misalkan dalam suatu ruangan, pada sebuah gedung atau sebuah warnet [2]. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan untuk memakai bersama sumber daya (misalnya *printer*) dan saling bertukar informasi. Sebuah LAN dapat terhubung dengan jaringan lain, misal dengan LAN lain atau terhubung dengan *internet*. Koneksi dengan LAN lain dapat dilakukan via perangkat perantara, seperti *router*, *modem*, *switch* dan sebagainya.
- b) *Metropolitan Area Network* (MAN)
Jenis jaringan komputer MAN ini adalah suatu jaringan komputer dalam suatu kota dengan transfer data berkecepatan tinggi yang menghubungkan suatu lokasi seperti sekolah, kampus, perkantoran dan pemerintahan [3]
- c) *Wide Area Network* (WAN)
Jaringan Wide Area Network (WAN) mempunyai cakupan terluas, bahkan dapat dikatakan mencakup seluruh dunia. Jaringan ini sendiri dapat dihubungkan dengan menggunakan satelit dan media kabel *fibre optic* [4].

2. Perangkat Keras Jaringan

Beberapa perangkat keras yang umum dan penting dalam membuat jaringan adalah kabel, kartu jaringan, *hub* atau *switch*, *router* dan modem.

- a) Kabel
Kabel merupakan penghantar arus dari dan ke sebuah perangkat jaringan yang lain [2]. Kabel merupakan salah satu bagian yang terpenting dalam media koneksi antara komputer dengan komputer lainnya. Terdapat beberapa jenis kabel yang sering digunakan sebagai media komunikasi jaringan. Terdapat tiga jenis kabel yang biasa digunakan dalam komunikasi data yang dikenal secara umum dan sering digunakan untuk jaringan LAN, yaitu *Coaxial*, *Twisted pair* dan *fibre optic*.
- b) *Switch*

Secara umum fungsi *switch* mirip dengan fungsi *hub* yang sudah lebih dulu ada. Namun jumlah perangkat jaringan yang dapat di koneksikan dengan *switch* jauh lebih banyak dibandingkan *hub* [2]. *Switch* bekerja dengan mempelajari alamat hardware host tujuan, sehingga informasi data yang dikirim bisa langsung dikirim ke *host* tujuan. *Switch* juga di kembangkan untuk mendukung kecepatan transfer data diatas 100 Mbps.

- c) *Router*
Router adalah sebuah perangkat yang berfungsi untuk menghubungkan dua jaringan atau lebih. *Router* dapat menghubungkan jaringan dengan topologi fisik dan topologi logika yang berbeda [2]. *Router* merupakan perangkat yang penting pada jaringan sebesar *internet*. Paket data diteruskan ke jaringan lain berkat *protocol routing* yang di tanamkan pada *router*.
- d) *Modem*
Modem (Modulator Demodulator) merupakan perangkat yang dapat digunakan untuk melakukan konversi sinyal digital menjadi sinyal analog, atau sebaliknya [2]. *Modem* digunakan untuk menghubungkan komputer dengan *internet*.

3. Aplikasi Penunjang Monitoring

- a) Nagios
Nagios merupakan salah satu aplikasi open source untuk network monitoring dan memiliki banyak plugins yang dapat digunakan untuk memaksimalkan proses monitoring perangkat jaringan yang ada. Beberapa fitur yang dimiliki Nagios seperti monitoring, alert, report, memantau resource CPU load, memory, status up/down, up time, data traffic, bandwidth dari perangkat [5].

Nagios digunakan untuk memonitor server dan aplikasi yang berjalan di jaringan. Alat ini dapat memonitor status perangkat dan dapat melakukan pemeriksaan status dan memberi tahu ketika terjadi masalah dalam jaringan. Penggunaan plugin eksternal membantu memberitahu manajer jaringan tentang masalah di jaringan [6].

- b) Nagvis
NagVis (www.nagvis.org) merupakan aplikasi tambahan pada sistem manajemen jaringan Nagios. NagVis berfungsi memvisualisasikan data Nagios [7].

Nagios digunakan untuk memonitor server dan aplikasi yang berjalan di jaringan. Alat ini dapat memonitor status perangkat dan dapat melakukan

pemeriksaan status dan memberi tahu ketika terjadi masalah dalam jaringan. Penggunaan plugin eksternal membantu memberitahu manajer jaringan tentang masalah di jaringan (Renita & Elizabeth, 2018).

- b) Nagvis
NagVis (www.nagvis.org) merupakan aplikasi tambahan pada sistem manajemen jaringan Nagios. NagVis berfungsi memvisualisasikan data Nagios Saputra dkk (2017).

III. METODE PENELITIAN

1. Analisa Penelitian

- a) Analisa Kebutuhan
Untuk dapat membuat perangkat *server* berfungsi sebagai *Network Monitoring System* diperlukan PC yang terinstall OS Ubuntu *Server* serta nagios itu sendiri sebagai aplikasi *monitoring* dan *plugin* nagvis yang nantinya akan digunakan sebagai *dashboard* yang dapat menampilkan informasi dari masing-masing jaringan dan *server* yang di monitor.
- b) Desain
Dalam implementasi *Network Monitoring System* ini dan dengan telah adanya *server* yang disediakan, maka tidak merubah desain jaringan yang sudah ada karena dalam implementasi ini hanya membutuhkan IP *address* yang disetting saat melakukan penginstalan *Operating System* (OS) dalam hal ini Ubuntu *Server*.
- c) Testing
Berhasil tidaknya dalam implementasi *Network Monitoring System* ini dipengaruhi beberapa faktor yang dapat menunjang keberhasilan baik dari segi infrastruktur atau *hardware* maupun dari segi *software* itu sendiri. Dari segi aplikasi setelah menginstal nagios harus benar-benar tahu akan menambahkan *host* apa saja, dalam hal ini nagios akan diberi akses untuk memonitor baik itu perangkat jaringan maupun *server*.
- d) Implementasi
Untuk pengimplementasiannya penulis akan menginstal di salah satu perangkat komputer yang telah disediakan oleh Divisi Teknologi Informasi PT. PELNI (Persero), untuk langkah-langkahnya terlebih dahulu akan melakukan penginstalan Ubuntu *Server*, pada saat penginstalan Ubuntu penulis juga akan menentukan IP *Address* yang digunakan untuk *server monitoring* tersebut dan selanjutnya akan menginstal Nagios beserta *plugin* Nagvis, pada saat penginstalan inilah akan menentukan sistem apa saja yang akan dimonitor,

dan fitur apa saja yang akan disediakan dengan melakukan konfigurasi di dalam aplikasi Nagios dan Nagvis.

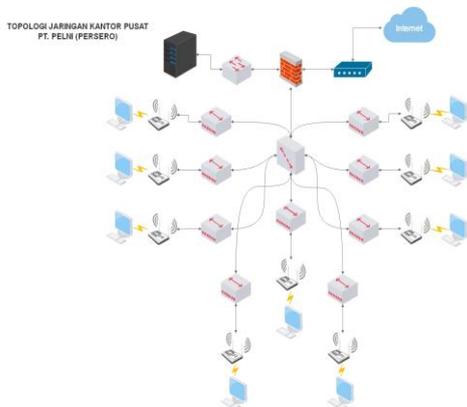
2. Metode Pengumpulan Data

- a) Observasi
Penulis melakukan pengumpulan data yang di peroleh dengan cara pengamatan langsung dengan melakukan riset kurang lebih 1 (satu) bulan di Divisi Teknologi Informasi PT. PELNI (Persero) yang bertujuan untuk mendapatkan gambaran secara luas mengenai infrastruktur jaringan yang sudah ada.
- b) Wawancara
Melakukan wawancara langsung ke Mgr. Operasional TI dan Spv. Adm Jaringan, *Hardware & Data Center* untuk mengetahui secara detail sistem yang berjalan dan permasalahan yang sering terjadi di Divisi Teknologi Informasi PT. PELNI (Persero).
- c) Studi Pustaka
Untuk mendukung pembuatan sistem monitoring ini, dilakukan studi pustaka dengan mengumpulkan bahan dari beberapa sumber, seperti media *internet*, jurnal dan beberapa buku referensi dengan tujuan agar dapat dijadikan sebagai acuan pembahasan dalam masalah ini sehingga terbentuk sebuah karya ilmiah yang baik.

IV. HASIL DAN PEMBAHASAN

1. Topologi Jaringan Usulan

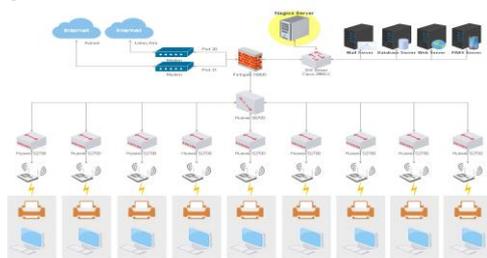
Berdasarkan pada latar belakang masalah yang ada dan dengan diimplementasikan sebuah perangkat untuk melakukan *monitoring* tidak mengubah topologi jaringan yang sudah berjalan.



Sumber: Penelitian, 2019
Gambar 1. Topologi Jaringan Usulan

2. Skema Jaringan

Pada skema jaringan usulan penulis menambahkan perangkat yang digunakan untuk melakukan monitoring. Skema jaringan yang diusulkan adalah sebagai berikut:



Sumber: Penelitian, 2019
Gambar 2. Skema Jaringan Usulan

3. Keamanan Jaringan

Keamanan jaringan merupakan hal yang sangat penting dalam melindungi dan mencegah adanya tindakan dari pihak lain yang tidak diinginkan. Keamanan jaringan yang digunakan pada PT. PELNI (Perseo) antara lain *firewall* dan antivirus symantec serta metode *security* WPA2-PSK untuk jaringan *wireless*.

a) Firewall

Untuk jaringan *internet* terdapat sebuah perangkat *firewall* yang berfungsi untuk mengatur otorisasi pada lalu lintas jaringan komputer yang dianggap aman untuk di lalui dan mencegah terhadap jaringan yang dianggap tidak aman. Perangkat *firewall* yang di gunakan di PT. PELNI (Persero) merupakan sebuah perangkat keras dengan tipe Fortigate 1500D.

b) Antivirus

PT. PELNI (Persero) memiliki Lisensi Antivirus Symantec untuk masing-masing komputer yang digunakan oleh karyawan, dimana antivirus ini sangat baik digunakan untuk melindungi komputer dari virus dan program perusak lain yang memiliki kemungkinan untuk dapat membahayakan keamanan jaringan yang ada pada PT. PELNI (Persero). Antivirus Symantec tersebut juga digunakan layaknya seperti *firewall* untuk melindungi dari serangan yang ada dalam jaringan maupun aktivitas karyawan yang berpotensi merusak, baik disengaja maupun tidak.

4. Rancangan Aplikasi

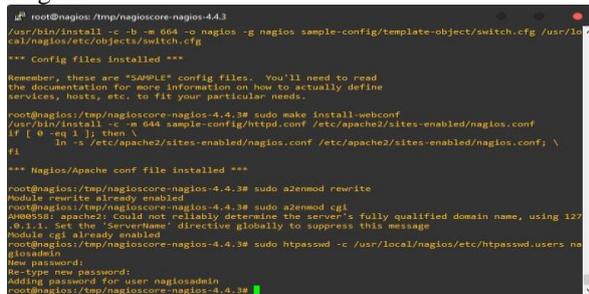
Dalam membangun sistem *monitoring* dibutuhkan sebuah perangkat *server* yang terinstall sistem operasi dimana penulis menggunakan Sistem operasi linux ubuntu *server* 16.04 dengan sistem monitoring Nagios Core 4.4 dan *plugin* Nagvis 1.9. Nagios ini tidak bisa berjalan sendiri sehingga memerlukan elemen-elemen yang terlibat di dalamnya seperti Apache sebagai *Web Server* dan *database* Mysql.

a) Instalasi Nagios

Untuk instalasi Nagios Core 4.4 dan *plugin* Nagvis 1.9 dengan melakukan download *file* installasinya terlebih dahulu dan melakukan instalasi Nagios. Untuk melakukan download dengan menggunakan *command* berikut:

```
$ cd /tmp
$ wget -O nagioscore.tar.gz
https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.3.tar.gz
$ tar xzf nagioscore.tar.gz
$ sudo apt-get install -y autoconf gcc libc6 make
wget unzip apache2 php libapache2-mod-php7.0
libgd2-xpm-dev
$ cd /tmp/nagioscore-nagios-4.4.3/
$ sudo ./configure --with-httpd-
conf=/etc/apache2/sites-enabled
$ sudo make all
$ sudo make install-groups-users
$ sudo usermod -a -G nagios www-data
$ sudo make install
$ sudo make install-daemoninit
$ sudo make install-commandmode
$ sudo make install-config
$ sudo make install-webconf
$ sudo a2enmod rewrite
$ sudo a2enmod cgi
$ sudo htpasswd -c
/usr/local/nagios/etc/htpasswd.users nagiosadmin
$ sudo systemctl restart apache2.service
$ sudo systemctl start nagios.service
```

Dari file Nagios Core yang sudah didownload dapat langsung diinstall dan dalam tahap penginstallan ini akan menambahkan *username* dan *password* yang nantinya akan digunakan untuk login di aplikasi Nagios.

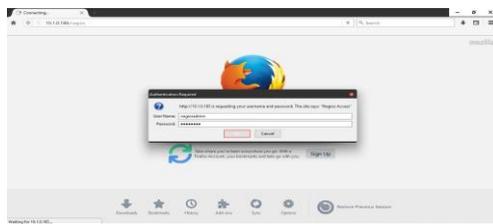


```
root@nagios:/tmp/nagioscore-nagios-4.4.3#  
/usr/bin/install -c -b -m 644 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg  
*** Config files installed ***  
Remember, these are *SAMPLE* config files. You'll need to read  
the documentation for more information on how to actually define  
services, hosts, etc. to fit your particular needs.  
root@nagios:/tmp/nagioscore-nagios-4.4.3# sudo make install-webconf  
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-enabled/nagios.conf  
if [ 0 -eq 1 ]; then \  
  ln -s /etc/apache2/sites-enabled/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \  
fi  
*** Nagios/Apache conf file installed ***  
root@nagios:/tmp/nagioscore-nagios-4.4.3# sudo a2enmod rewrite  
Module rewrite already enabled  
root@nagios:/tmp/nagioscore-nagios-4.4.3# sudo a2enmod cgi  
Module cgi already enabled  
root@nagios:/tmp/nagioscore-nagios-4.4.3# sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin  
New password:  
Re-type new password:  
Adding password for user nagiosadmin  
root@nagios:/tmp/nagioscore-nagios-4.4.3#
```

Sumber: Penelitian, 2019

Gambar 3. Instalasi Nagios

Setelah proses instalasi selesai kita dapat membuka *browser* yang kita miliki untuk mengakses aplikasi Nagios dengan mengetikan IP *address* dari *server monitoring* yaitu <http://10.1.0.185/nagios> seperti gambar berikut:



Sumber: Penelitian, 2019

Gambar 4. Halaman Login Nagios

Username dan *password* untuk aplikasi Nagios telah kita buat saat proses instalasi. Setelah sesuai memasukkan *username* dan *password* maka Nagios untuk *monitoring system* sudah dapat digunakan, adapun tampilan awal dari nagios adalah sebagai berikut:



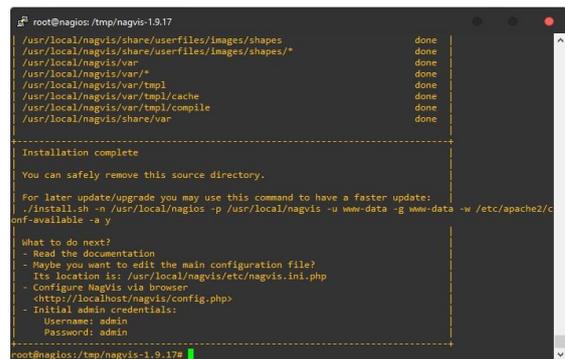
Sumber: Penelitian, 2019

Gambar 5. Dashboard Nagios

b) Instalasi Nagvis

Selanjutnya adalah melakukan instalasi *plugin* Nagvis 1.9 yang akan digunakan untuk membuat *dashboard monitoring* dengan menggunakan perintah:

```
$ cd /tmp/  
$ wget 'http://www.mathias-kettner.de/download/mk-livestatus-1.2.8.tar.gz'  
$ tar xzf mk-livestatus-1.2.8.tar.gz  
$ cd mk-livestatus-1.2.8  
$ ./configure  
$ make install  
$ cd /tmp/  
$ wget http://www.nagvis.org/share/nagvis-1.9.17.tar.gz  
$ tar xvzf nagvis-1.9.17.tar.gz  
$ cd nagvis-1.9.17/  
$ chmod +x install.sh  
$ ./install.sh
```



```
root@nagios:/tmp/nagvis-1.9.17#  
/usr/local/nagvis/share/userfiles/images/shapes done  
/usr/local/nagvis/share/userfiles/images/shapes/* done  
/usr/local/nagvis/var done  
/usr/local/nagvis/var/* done  
/usr/local/nagvis/var/tmp1 done  
/usr/local/nagvis/var/tmp1/cache done  
/usr/local/nagvis/var/tmp1/compile done  
/usr/local/nagvis/share/var done  
Installation complete  
You can safely remove this source directory.  
For later update/upgrade you may use this command to have a faster update:  
./install.sh -m /usr/local/nagvis -u www-data -g www-data -w /etc/apache2/conf-available -a y  
What to do next?  
- Read the documentation  
- Maybe you want to edit the main configuration file?  
  Its location is: /usr/local/nagvis/etc/nagvis.ini.php  
- Configure Nagvis via browser  
  <http://localhost/nagvis/config.php>  
- Initial admin credentials:  
  Username: admin  
  Password: admin  
root@nagios:/tmp/nagvis-1.9.17#
```

Sumber: Penelitian, 2019

Gambar 6. Instalasi Nagvis

Dari proses instalasi nagvis secara otomatis akan membuat *username* dan *password* yang akan di gunakan untuk login kedalam aplikasi nagvis. Setelah proses instalasi nagvis selesai kita dapat membuka *browser* yang kita miliki untuk mengakses aplikasi nagvis dengan mengetikan IP *address* dari *server monitoring* yaitu <http://10.1.0.185/nagvis> seperti gambar berikut:



Sumber: Penelitian, 2019

Gambar 7. Dashboard Nagvis

c) Konfigurasi *Host* Nagios

Selanjutnya perlu dilakukan konfigurasi Nagios, untuk konfigurasi terletak pada direktori /usr/local/nagios/etc. Semua konfigurasi Nagios tersimpan di dalam direktori /usr/local/Nagios/etc/server dan perlu dilakukan penambahan file routercabang.cfg dan serverpelni.cfg pada direktori /usr/local/nagios/etc/server. Semua file konfigurasi tersebut akan di baca oleh aplikasi Nagios dan nantinya akan di tampilkan di dashboard Nagios yang juga dapat diakses oleh nagvis.

```
define host {
    use generic-host ; Name of host template$
    host_name Router-Ambon
    hostgroups cabang
    alias router-ambon
    address 10.0.0.33
    parents Router-Cabang
    check_command check-host-alive
    max_check_attempts 10
    contact_group nagiospelni
    notification_interval 300
    notification_period 24x7
    notification_options d,u,r
}

define host {
    use generic-host ; Name of host template$
    host_name Router-Ambon-Port
    hostgroups cabang
    alias router-ambon-port
    address 10.0.0.33
    parents Router-Cabang
    check_command check-host-alive
    max_check_attempts 10
    contact_group nagiospelni
    notification_interval 300
    notification_period 24x7
    notification_options d,u,r
}

define host {
    use generic-host ; Name of host template$
    host_name Router-Amanan
    hostgroups cabang
    alias router-amanan
```

Sumber: Penelitian, 2019

Gambar 8. Konfigurasi *Host* Nagios

d) Konfigurasi *Host* Nagvis

File konfigurasi map yang sudah dibuat tersimpan di dalam direktori nagvis /usr/local/nagvis/etc/ maps, dari file ini kita dapat melakukan konfigurasi kembali dengan menambahkan host yang sudah terdaftar di aplikasi Nagios. Map yang sudah dibuat bisa ditambahkan background yang nanti akan ditampilkan melalui dashboard yang sudah dibuat.

```
define global {
    alias=Cabang
    object_id=0
    map_image=pelembicabang73ag.jpg
    zoom=fill
    grid_show=0
    header_show=1
}

define host {
    host_name=Router-Sorong
    x=100
    y=50
    object_id=25433
    icon=tsad_geo
    view_type=icon
    icon_size=35
    label_text=SORONG
    label_x=10
    label_y=28
    label_style=bold
    label_border=transparent
}

define host {
    host_name=Router-Manokwari
    x=100
    y=25
    object_id=68ec97
    view_type=icon
    icon_size=35
    label_text=Manokwari
    label_border=transparent
    label_show=1
}
```

Sumber: Penelitian, 2019

Gambar 9. Konfigurasi *Host* Nagvis

5. Pengujian Jaringan

a) Pengujian Jaringan Awal

Dalam pengujian jaringan awal yang dilakukan menggunakan *command prompt* dengan melakukan *test ping* ke ke perangkat *server* yang ada di *data*

center dan *router* yang ada di kantor cabang. Pengujian ini dilakukan untuk mengetahui status *host* yang akan di monitor.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NOPS>ping 10.1.0.185

Pinging 10.1.0.185 with 32 bytes of data:
Reply from 10.1.0.185: bytes=32 time=1ms TTL=64
Reply from 10.1.0.185: bytes=32 time=1ms TTL=64
Reply from 10.1.0.185: bytes=32 time=1ms TTL=64

Ping statistics for 10.1.0.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NOPS>ping 10.3.1.1

Pinging 10.3.1.1 with 32 bytes of data:
Reply from 10.3.1.1: bytes=32 time=14ms TTL=251
Reply from 10.3.1.1: bytes=32 time=14ms TTL=251
Reply from 10.3.1.1: bytes=32 time=13ms TTL=251

Ping statistics for 10.3.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 14ms, Average = 13ms
```

Sumber: Penelitian, 2019

Gambar 10. Pengujian Status *Host*

b) Pengujian Jaringan Akhir

Untuk pengujian jaringan akhir menggunakan aplikasi Nagios sbgai *network monitoring* dan Nagvis sebagai *dashboard* yang sudah penulis rancang pada pembahasan sebelumnya. Pengujian dilakukan dengan menambahkan *host* untuk dapat dimonitoring melalui aplikasi Nagios, terlihat dalam gambar dibawah *host* yang sudah ditambahkan akan menampilkan status (*Up*) apabila *host* dalam keadaan aktif dan menampilkan status (*Down*) apabila *host* dalam keadaan tidak aktif.

Host**	Status**	Last Check**	Duration**	Status Information
Cabang-Malassar	DOWN	04-12-2019 13:54:48	0d 0h 1m 0s	(Host check timed out after 30.01 seconds)
Cabang-Sorong	UP	04-12-2019 13:54:56	0d 0h 1m 2s+	PING OK - Packet loss = 0%, RTT = 56.71 ms
Cabang-Sarabaya	UP	04-12-2019 13:55:04	0d 0h 1m 2s+	PING OK - Packet loss = 0%, RTT = 14.48 ms
Server-DB	UP	04-12-2019 13:55:56	0d 0h 1m 2s+	PING OK - Packet loss = 0%, RTT = 0.77 ms
Server-MAL	UP	04-12-2019 12:43:00	47d 0h 4m 19s	PING OK - Packet loss = 0%, RTT = 0.44 ms
Server-NAGIOS	UP	04-12-2019 12:43:01	211d 15h 32m 7s	PING OK - Packet loss = 0%, RTT = 0.10 ms
Server-PANEL	UP	04-12-2019 13:55:29	0d 0h 1m 2s+	PING OK - Packet loss = 0%, RTT = 1.81 ms
Server-WEB	UP	04-12-2019 12:38:12	19d 4h 47m 39s	PING OK - Packet loss = 0%, RTT = 1.51 ms

Sumber: Penelitian, 2019

Gambar 11. Daftar *Host* Nagios

Untuk tampilan *dashboard* yang sudah dibuat menampilkan status *host* sesuai yang ada di aplikasi Nagios. Nagvis yang dibuat akan secara terus menerus mengecek semua status *host* yang sudah ditambahkan ke dalam *dashboard*. Apabila ada perubahan status yang ada di Nagios maka *host* yang ada di *dashboard* nagvis akan mengikuti.



Sumber: Penelitian, 2019

Gambar 12. *Dashboard Host* Nagvis

Dari *dashboard* di atas dapat terlihat bahwa status *host* cabang makassar mengalami (*Down*) sedangkan status cabang surabaya dan sorong dalam keadaan aktif (*Up*) sesuai data *host* yang diterima dari aplikasi Nagios. Dengan adanya *dashboard* ini dapat memudahkan *administrator* dalam melakukan pemantauan perangkat jaringan yang ada di cabang. Fungsionalitas Nagios untuk *monitoring* jaringan cabang ataupun *server* berjalan dengan normal, hal ini dibuktikan dengan terdapatnya informasi status *host* dari setiap perangkat yang di *monitor*.

V. KESIMPULAN

Berdasarkan hasil analisa jaringan komputer yang ada pada PT. PELNI (Persero), didapatkan beberapa hasil sebagai berikut:

1. Sistem jaringan yang ada di PT. PELNI (Persero) dirancang dengan baik dan didukung oleh *hardware* dan *software* yang memadai, namun dari banyaknya perangkat jaringan dan *server* yang digunakan belum adanya sistem *monitoring* yang bisa digunakan untuk melakukan pemantauan terhadap semua perangkat tersebut. Sehingga apabila perangkat jaringan ataupun *server* mengalami *down* perlu dilakukan pengecekan secara manual.
2. Dengan menggunakan Nagios sebagai *network monitoring system* dan Nagvis digunakan sebagai *dashboard* seorang *administrator* jaringan dapat mengetahui dengan cepat apabila terjadi masalah pada perangkat jaringan dan *server*, karena dengan sistem *monitoring* ini dapat digunakan untuk melakukan pemantauan seluruh *host* yang terkoneksi ke dalam jaringan.

REFERENASI

Disusun dan diberi nomor urut berdasarkan urutan kutipan. Penulisan pustaka: nama penulis (tanpa gelar), tahun, judul, penerbit, dan kota penerbit. Berikut adalah contoh penulisan daftar pustak/referensi:

- [1] Habibullah, T., & Arnaldy, D. (2016). Implementasi *Network Monitoring System* Nagios dengan *Event Handler* dan Notifikasi *Telegram Messenger*. *MULTINETICS*, 2(1), 13–23
- [2] Primartha, R. (2019). *Manajemen Jaringan Komputer Teori dan Praktik*. Bandung: Informatika.
- [3] Wongkar, S., Sinsuw, A. A. E., & Najooan, X. (2015). Analisa Implementasi Jaringan Internet dengan Menggabungkan Jaringan LAN dan WLAN di Desa Kawangkoan Bawah wilayah Amurang II. *Jurnal Teknik Elektro Dan Komputer*, 4(6), 62–68.
- [4] Suwandhi, A., & Erpin, J. (2015). Analisa Sistem Pengaman Data Jaringan Berbasis VPN. *Stmik Ikmi*, 10(18), 220.
- [5] Oktivasari, P., & Habibullah, T.-. (2017). Kajian Network Monitoring System Menggunakan Nagios Dengan Whatsapp Sebagai Notifikasi Alert. *Jurnal Komunika : Jurnal Komunikasi, Media Dan Informatika*, 6(3), 34–43
- [6] Renita, J., & Elizabeth, N. E. (2018). Network's server monitoring and analysis using Nagios. *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017, 2018-Janua(March)*, 1904–1909
- [7] Saputra, E., Mauladi, M., & Sutrasno, T. (2017). Analisis dan Pemetaan Nilai Aksesibilitas *Hotspot Area* di Kampus Mendalo Universitas Jambi Menggunakan Sistem Informasi Geografis (Sig). *Jurnal Ilmiah Universitas Batanghari Jambi*, 17(2), 11–16.
- [8] Verdi Yasin, Anindra Ramdhan Nugraha, Muhammad Zarlis, Ifan Junaedi (2018) "Smart system of fast internet access development using backbone network method" *JISICOM (Journal of Information System, Informatics and Computing)* e-ISSN: 2597-3673, p-ISSN: 2579-5201. Vol.2 No.2 (2018),pp.26-34
<http://journal.stmikjayakarta.ac.id/index.php/jisicom/article/view/198>