Nagios®

Only the NSA monitors more

Mis on Nagios?

- Nagios on süsteemi ja võrgu seire rakendus.
- Nagios jälgib seadmeid ja teenuseid ning teavitab, nii vigade tekkest, kui normaalse olukorra taastumisest.

Nõuded OS-ile ja arvutiarhitektuurile

- Linux OS
- Debian
- Ubuntu
- Red Hat
- Suse
- Fedora
- UNIX OS
- FreeBSD
- OpenBSD
- NetBSD
- Solaris
- MAC X OS

Nagios töötab erineva arhitektuuriga riistvaral:

- x86, amd64, (PC)
- PowerPC (MAC), ALPHA, SPARC (SUN),
- AI64 Itanium (HP-UX, AIX)

Nõuded süsteemile

- Linux või UNIX OS, millel on C kompilaatori tugi.
- TCP/IP protokollide tugi - enamiku rakenduste kontroll käib üle TCP/IP võrgu.
- Veebiliidese jaoks on vajalik:
  - veebserver (soovitavalt Apache)
  - Thomas Boutell's gd library versioon 1.6.3 või uuem, mis on vajalik „statusmap“ ja „ trends CGI“ liideste tööks.

Litsentseerimise poliitika

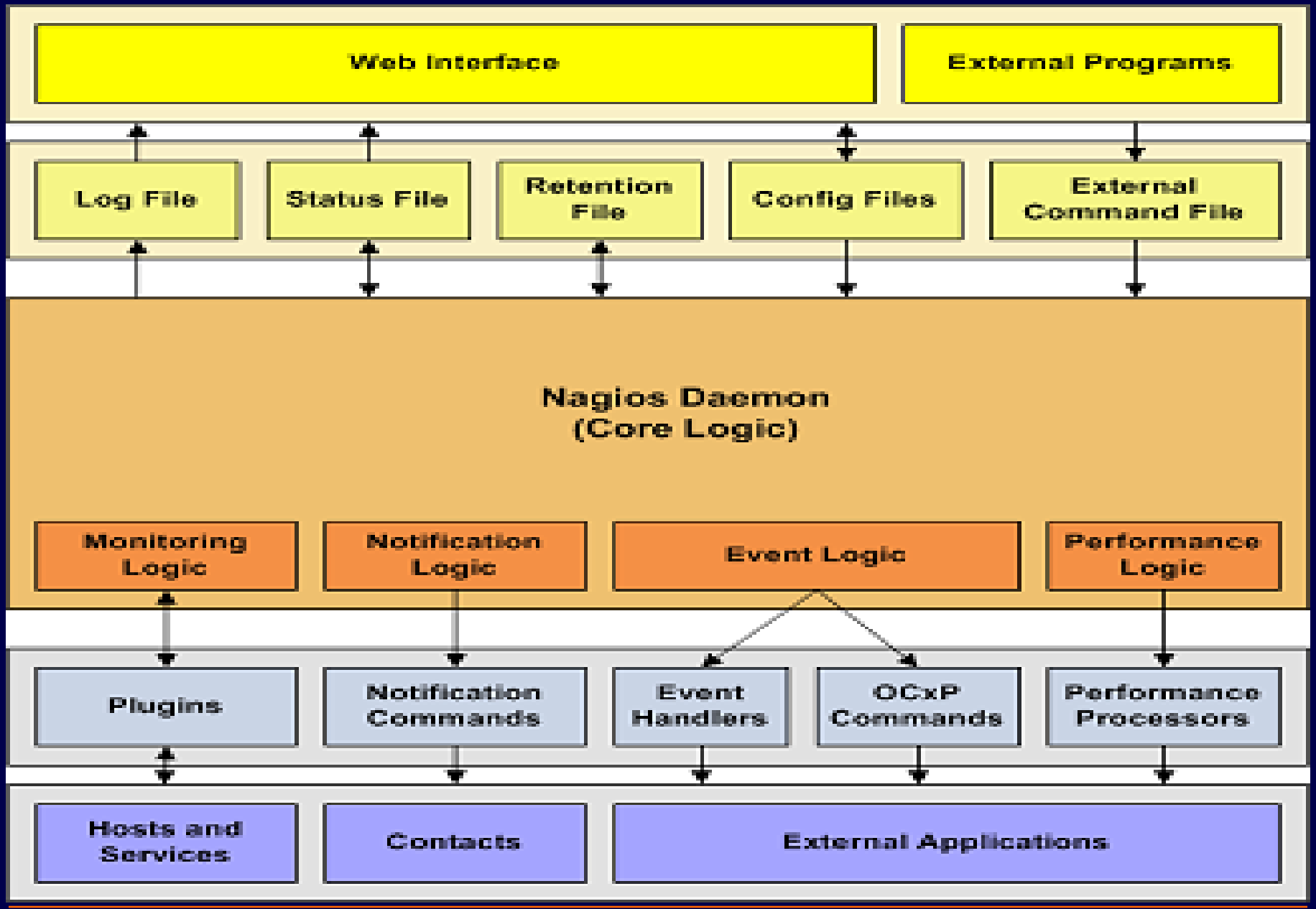
- GNU – General Public License ver. 2
- Nagios rakendust võib:
  - kopeerida
  - muuta
  - luua eriversioone (kui tegevus ei lähe vastuollu Nagiose litsentsitingimustega)

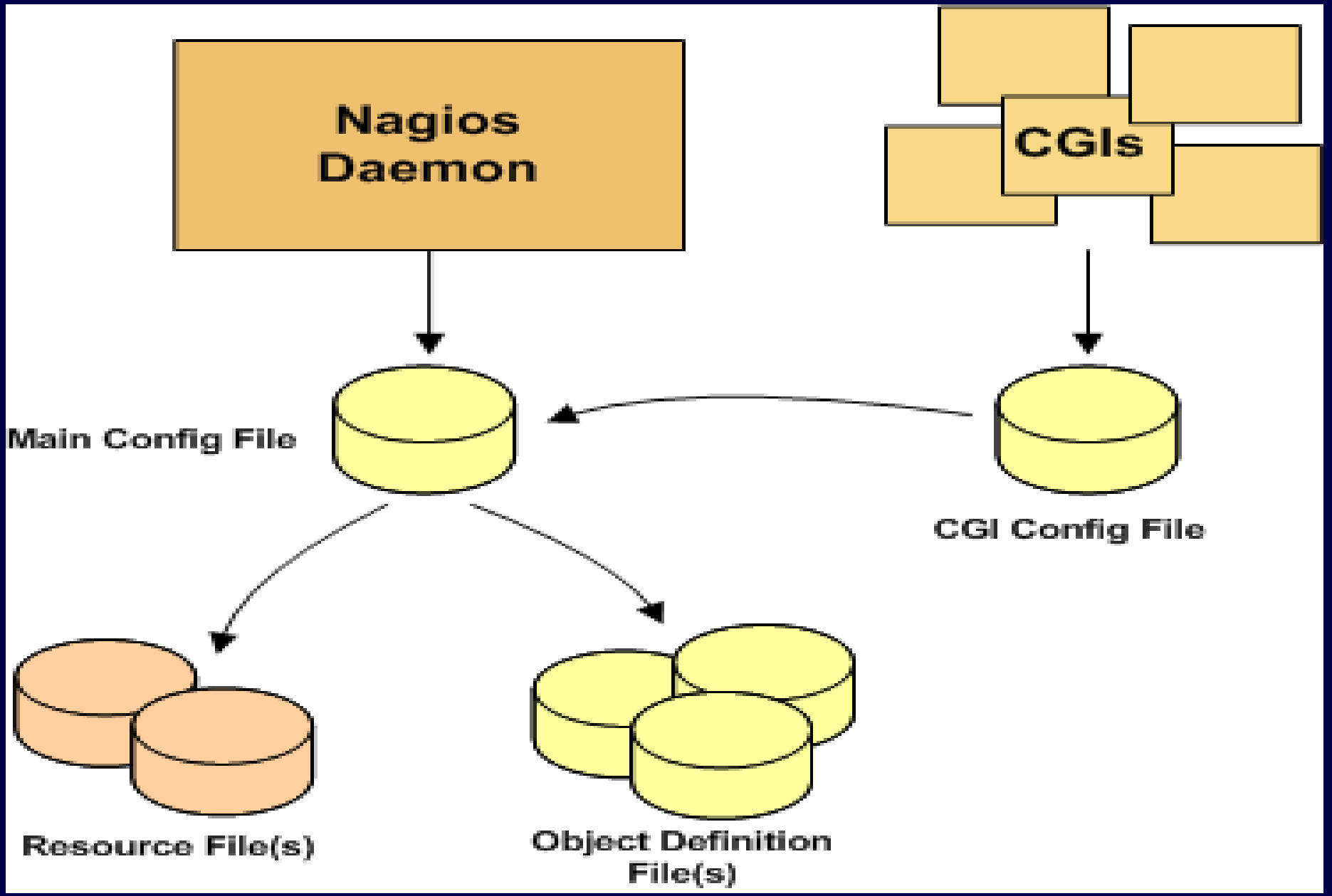
Nagios võimaldab

- Võrgurakenduste seiret (SMTP, POP3, HTTP, NNTP, PING, IMAP, SSH jne).
- Seadmete ressursside seiret (CPU koormus, ketta kasutus, mälu kasutus jne).
- Paralleelset rakenduste seiret.
- Automaatset logifailide uuendamist, vana logifaili sisu suunatakse arhiivi.
- Lisa (varu) seiresüsteemi tuge.
- Veebiliidest kus on võimalik jälgida seadmete, rakenduste, võrgu hetkeseisu; teadete ja probleemida ajalugu ning logifailide sisu jne.

Nagios sisaldab

- Lihtsaid vahendeid, mis võimaldavad kasutajal ise erinevaid seire skripte.
- Võimalust määrata võrgu seadmete hierarhiat, mis lihtsustab vigade lokaliseerimist. Võimaldab vahet teha seadmete ja teenustel, mis ei tööta või mis pole kättesaadavad seire süsteemile.
- Teadetesaatmise moodulit ja teadete saajate seadistus moodulit, mis saadab teate, kui probleem tekib või laheneb kasutades selleks e-posti, pager või muud kasutaja poolt määratud meetodit).
- Võimalust määrata seiresüsteemi käitumist rakenduse või seadme veateate korral, mis võimaldab kiiremat tegutsemist vea korral.


Web Interface
External Programs
Log File
Status File
Retention File
Config Files
External Command File
Nagios Daemon
(Core Logic)
Monitoring Logic
Notification Logic
Event Logic
Performance Logic
Plugins
Notification Commands
Event Handlers
OCxP Commands
Performance Processors
Hosts and Services
Contacts
External Applications

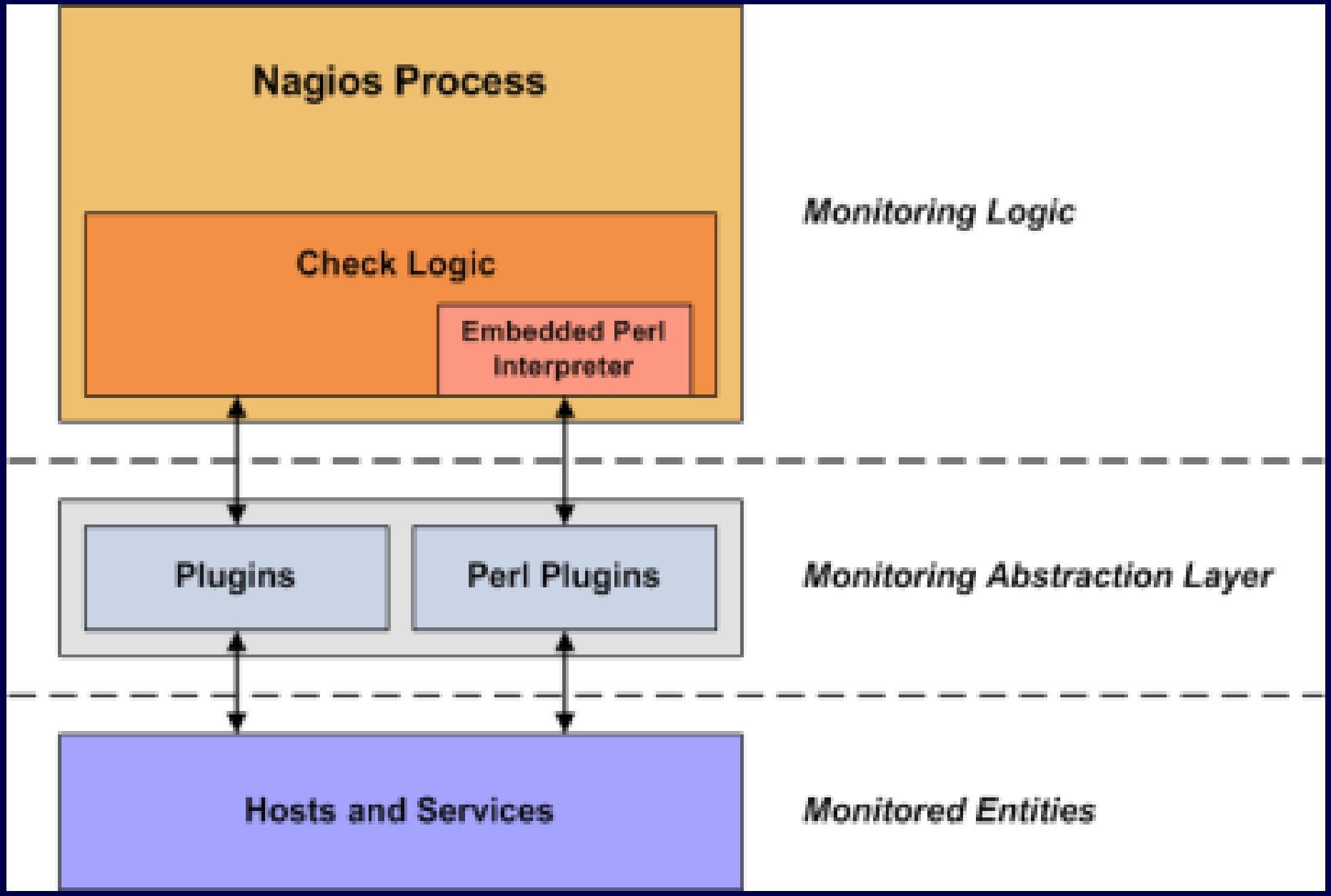

Nagios
Daemon
CGIs
Main Config File
CGI Config File
Resource File(s)
Object Definition
File(s)

Objektide liigid

- Teenused
- Teenuste grupid
- Seadmed
- Seadmete grupid
- Vastutavad isikud
- Vastutavate isikute grupid
- Ajaplaan
- Info teavituste eskalatsiooni kohta

Nagiose moodulid

- Nagiose põhirakendus ei sisalda skripte.
- Nagios teostab seiret läbi alamprogrammide.
- Pluginad teostavad seire ja tagastavad tulemuse.
- Pluginag koosnevad skriptidest (kirjutatud Perli või shell skriptis).
- Plugina vastuse peale Nagios reageerib vastavalt:
  - käivitades „events handlers“ mooduli
  - saates välja teate


Nagios Process
Check Logic
Embedded Perl Interpreter
Monitoring Logic
Plugins
Perl Plugins
Monitoring Abstraction Layer
Hosts and Services
Monitored Entities

Nagiose pluginatest veel...

- Plugin tagastab Nagios demonile ühe neljast signaalist:
  - 0 – teenus on OK
  - 1 – teenus on HOIATUS tasemel
  - 2 – teenus on KRIITILINE
  - 3 – teenuse seisund TEADMATA
- Pluginaid pole täiesti eraldiseisvad programmid, nad on pigem nagu alammeetodid.
- Pluginaid saab käsurealt käivitada.

Lisa pluginaid saab...

- Osa pluginaid on kaasas Nagiosega
- Lisaks võib neid alla laadida:
  - Nagios Plugins Project: http://nagiosplug.sourceforge.net/
  - Nagios Downloads Page: http://www.nagios.org/download/
  - NagiosExchange.org: http://www.nagiosexchange.org/
- Pluginate kasutuse kohta saab infot käsuga ./plugina_nimi --help, mis tuleb käivitada käsurealt.

Nagiose makrod

- Makro käivitab vastava plugina koos makrosse defineeritud väärtusega.
- Seega, makrot võib vaadata kui täiendavat abstraktsioonitaset
- Makrod võivad ka makrodest koosneda, mis lisab veel paindlikkust.
- Makros saab defineerida iga pluginale või käsule HOIATUS ja KRIITILISE taseme väärtused.

On-Demand makro

- On-Demand makro puhul käsk sisaldab kindla hosti nime, kust infot käivitatav plugin küsib.

  $CONTACTEMAIL:john$ On-demand contact macro

  $CONTACTGROUPMEMBERS:linux-admins$ On-demand contactgroup macro

  $HOSTGROUPALIAS:linux-servers$ On-demand hostgroup macro

Tavaline makro

```
define service{
        host_name               linuxbox
        service_description     PING
        check_command           check_ping!
   200.0,80%!400.0,40%
        }
```

Custom Variable makro

- Kolmas tüüp on custom Variable makro, kus tavalist makrot täiendatakse näiteks MAC aadressiga, et küsi infot vaid kindla MAC-aadressiga seadme käest.
  - $_HOST*varname*$
  - $_SERVICE*varname*$
  - $_CONTACT*varname*$

```
define host{
    host_name                   linuxbox
    address                     192.168.1.1
    _MACADDRESS 00:01:02:03:04:05
    }
```

Piirangud makrode kasutamisel

- Päris suvalist pluginat ei saa kasutada suvalises makros.
- On olemas 10 peamist gruppi makrosid, millega saab rakendada iga ühes kindlaid pluginaid

Peamised makrode grupid

- Service checks
- Service notifications
- Host checks
- Host notifications
- Service event handlers and/or a global service event handler
- Host event handlers and/or a global host event handler
- OCSP command
- OCHP command
- Service performance data commands
- Host performance data commands

Seiremeetodid I

- Host check – seadme seire
  - teostatakse teatud ajaintervalli järel
  - tulemus võibolla kas:
    - UP – seade vastab OK
    - DOWN – seade ei vasta
      - KRIITILINE
      - UNREACHABLE

Seiremeetodid II

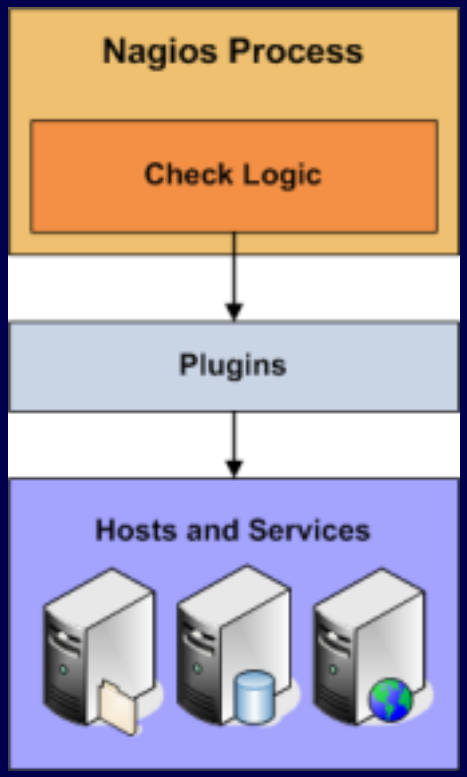
- Service check – teenuse, rakenduse seire
  - teostatakse teatud ajaintervalli järel
  - tulemus võibolla kas:
    - OK – teenus annab vastuse, mis vastav makros defineeritud OK väärtusvahemikule,
    - WARNING – teenus annab vastuse, mis vastav makros defineeritud WARNING väärtusvahemikule
    - UNKNOWN – teenust pole võimalik seirata, sest võrguühendus puudub
    - CRITICAL – teenus annab vastuse, mis vastav makros defineeritud CRITICAL väärtus vahemikule.

Seiremeetodid III

- Aktiivne seire
  - kasutatakse teenuste ja seadmete seires.
  - kontrolli algataja Nagiose seiresüsteem.
  - toimub regulaarselt graafiku alusel.
  - Enamikel juhtudes kasutatakse aktiivset seiret.

Seiremeetodid IV

- Aktiivne seire
  - Nagios rakendus käivitab plugina, mis teostab seadme või teenuse seire ja tagastav vastuse Nagios rakendusele, mis vastavalt kas saadab teate veakorral või käivitab Evend Handlersi.

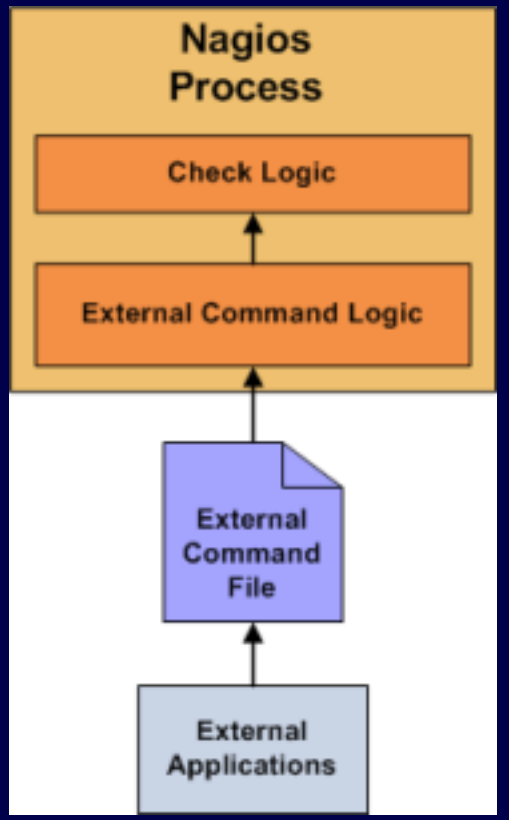


Seiremeetodid V

- Passiivne seire
  - teostatakse välise rakenduse poolt
  - tulemused saadetakse Nagiose seire süsteemile.
  - seire protsessi alustajaks pole Nagios rakendus vaid väline rakendus.
- Passiivset seiret kasutatakse kui:
  - andmeside kanal seiratava teenuse või seadmeni on asünkroonne.
  - pole võimalik efektiivne regulaarne graafiku alusel aktiivne seire.
  - seiratav teenus, või seade on tulemüüri taga
  - pole võimalik otse aktiivne seire.
  - tegemist on ebaregulaarselt toimuva sündmusega näiteks SNMP Trap teated
  - Kui tegemist on hajutatud, liiasusega seiresüsteemiga (keskne server on pasiiv- ja kohapealsed serverid on aktiivrežiimis).

Seiremeetodid VI

- Passiivne seire
- Väline rakendus kontrollib seadme või teenus staatust ja kirjutab tulemuse external command faili.
- Iga kord, kui Nagios loeb externel command faili ta tekitab korralduse lugeda faili uuesti mingi aja tagant.
- Ja edasine protsess kaasa arvatud perioodiliselt kas external command faili lugemine või pluginale teenuse kontrollimise korralduse andmine on sarnane aktiiv- ja passiivkontrolli korral.
- Edasine reageerimine on sama mis aktiivseire korral.
- Seega võib sama Nagios rakendus sama aegselt teostada nii aktiiv- kui passiivseiret.



Sündmustele reageerimine

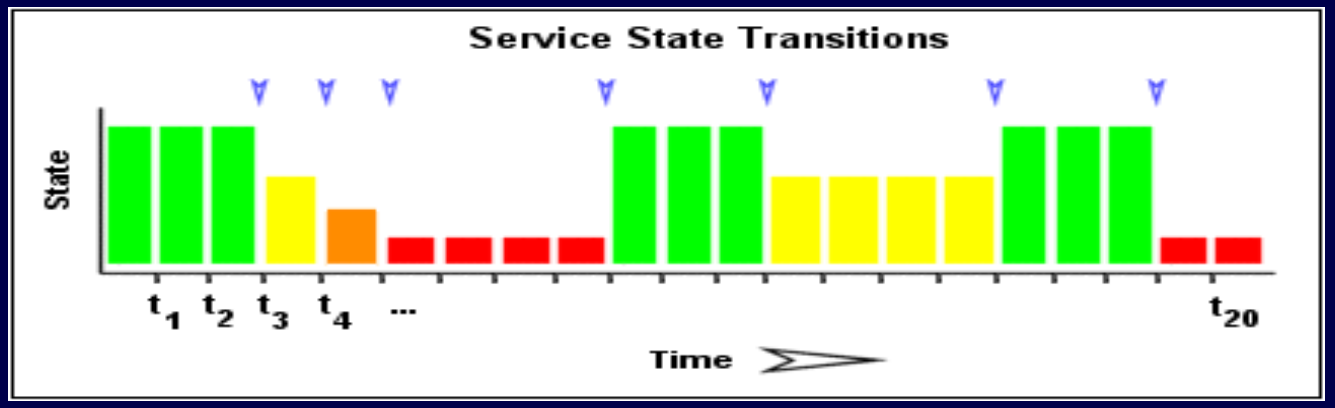
- Nagios saadab teateid vastavalt kontaktides ja kontaktigruppides defineeritule.
- Nagis versioon 3 on võimalik kasutada „scheduled downtime“ teenust, mis võimaldab planeeritud tööde korral mitte registreerida veateateid.

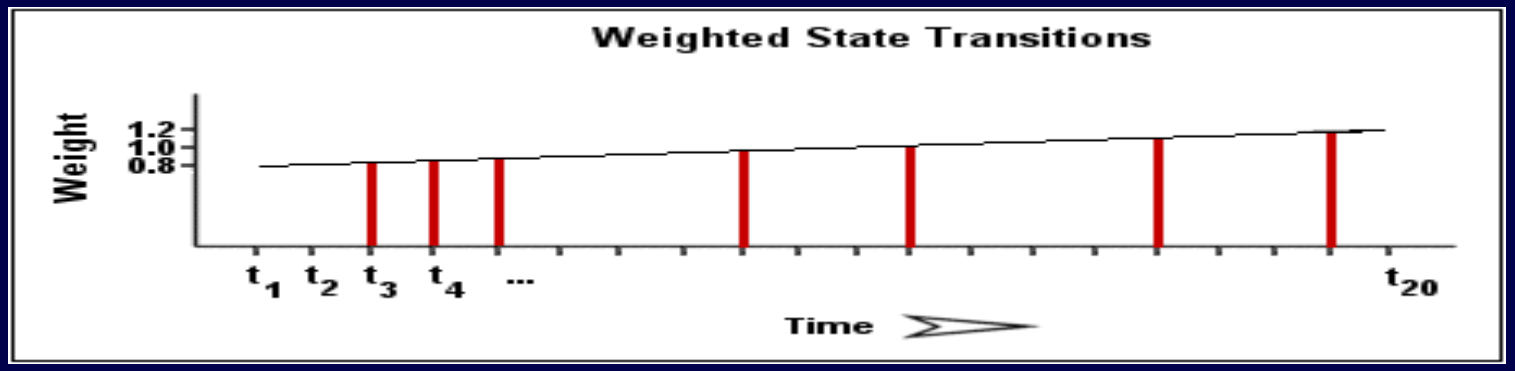
“HARD” ja “SOFT” seisund

- HARD seisundi muutusel saadetakse teade ja sündmust logitakse.
- SOFT seisundi muutusel logitakse, teadet ei saadeta.
- Näide: Kontrolli vastus on HOST maas. Kontrollitakse vähemalt 3 korda, siis pärast 1-st kontrolli läheb HOST SOFT olekusse ja pärast 3-ndat kontrolli, kui ikkagi on HOST maas läheb seade HARD olekusse.

„Detection and Handling of State Flapping“ teenus

- Võimaldab vältida teadete laviini, mis on tingitud teenustest, mis liiga tihti muudavad staatust.
- Nagios arvestab viimast 21 kontrolli ja analüüsib kas teenuse muutus on toimunud liiga sageli võrreldes eelmise 21 kontrolli vältel toimunud muutustega.





- (7 kindlaks tehtud teenuse seisund muutused / võimalikud 20 teenuse seisundi muutust) * 100 = 35 %.
- Näiteks, kui järgneval perioodil on teenuse muutuse osakaal alla 31%, mis on väiksem , kui 35%, siis Nagios teatab, et teenus STOP FLAPPING.
- Aga kui teenus oli eelnevalt non flapping ja nüüd läheb staatuse muutuse protsent üle 31%, siis Nagios teatab, et teenus START FLAPPING.

Nagiose “väljundid” I

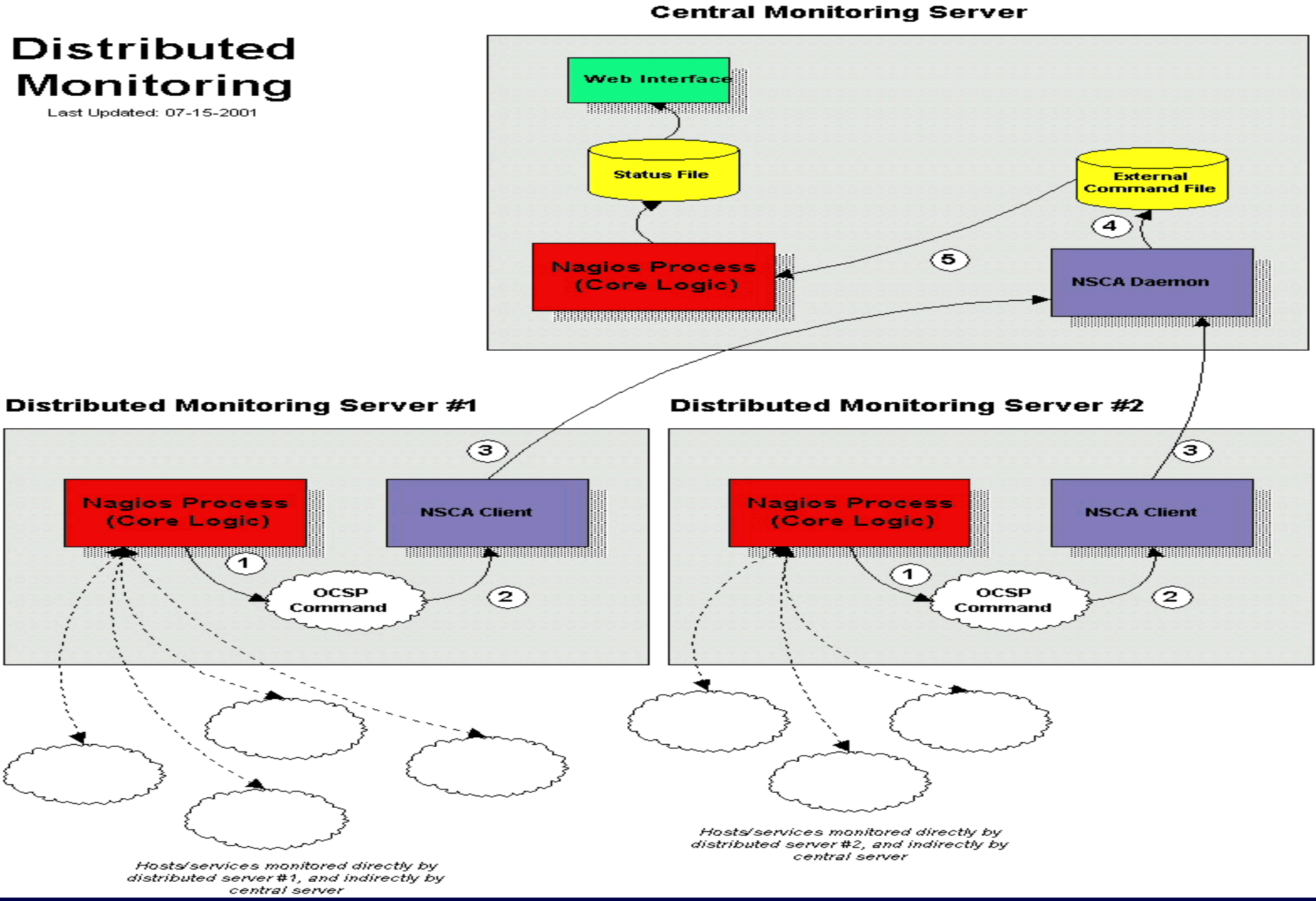
- Nagios võimaldab kasutada erinevaid teadete edastamise kanaleid.
- Tuleb vaid paigaldada ja seadistada vastav tarkvara.
- Näitena on toodud loetelu võimalikest teate edastamise kanalitest:
  - Email, Pager, Phone(SMS),
  - WinPopup message, Yahoo, ICQ, MSN instant message,
  - Audio alerts jne.

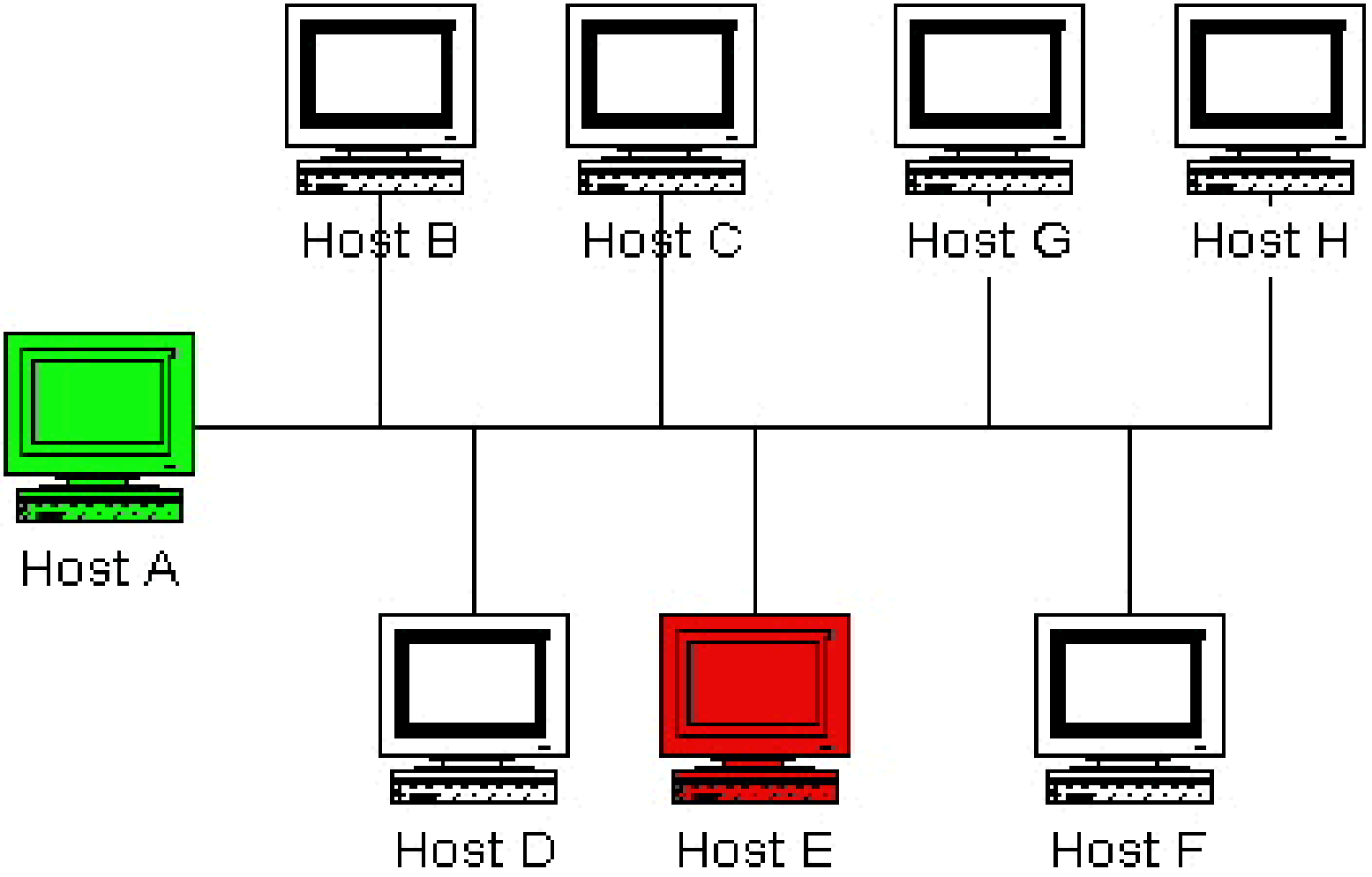
Nagiose “väljundid” II

- Käsurea käskude peale saab sõnumeid moodustada.
- E-postile saadetavate teadete asemel võib kasutada ka järgnevaid teenuseid:
- Gnokii (SMS software for contacting Nokia phones via GSM network)
- QuickPage (alphanumeric pager software)
- Sendpage (paging software)
- SMS Client (command line utility for sending messages to pagers and mobile phones)
- Festival – liides, mis võimaldab seire serveril teavitada sündmustest kõnes kõnesünteesi abil.
- Network Audio System (NAS) and rplay – projektid, mille abil on võimalik kõnesünteesi poolt tekitatud teade maha mängida kaugarvutis (administraatori arvuti).

Distributed Monitoring

Last Updated: 07-15-2001

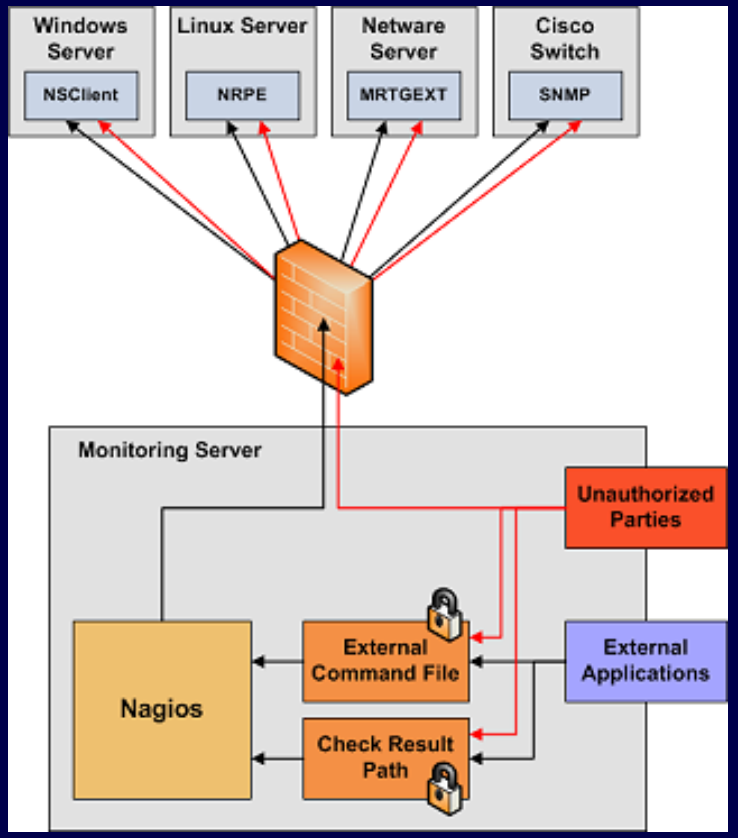




- A – master (põhi)seireserver
- E – slave (varu)seireserver

Nagiose turvalisus I

- Soovituslikult töötab Nagios iseseisvas seire serveris.
- Soovituslikult seireserveril puudub väljast otse juurdepääs.



Nagiose turvalisus II

- Nagios ei tööta ROOT kasutaja õigustes vaod omab näiteks kasutaja nagios õigusi ja kuulub kasutajate gruppi nagios.
- Vaikimisi saavad lugeda ja kirjutada check result path-i kasutajad nagios ja root, et välistada petteteadete saatmine Nagios seirerakendusele.

Nagiose turvalisus III

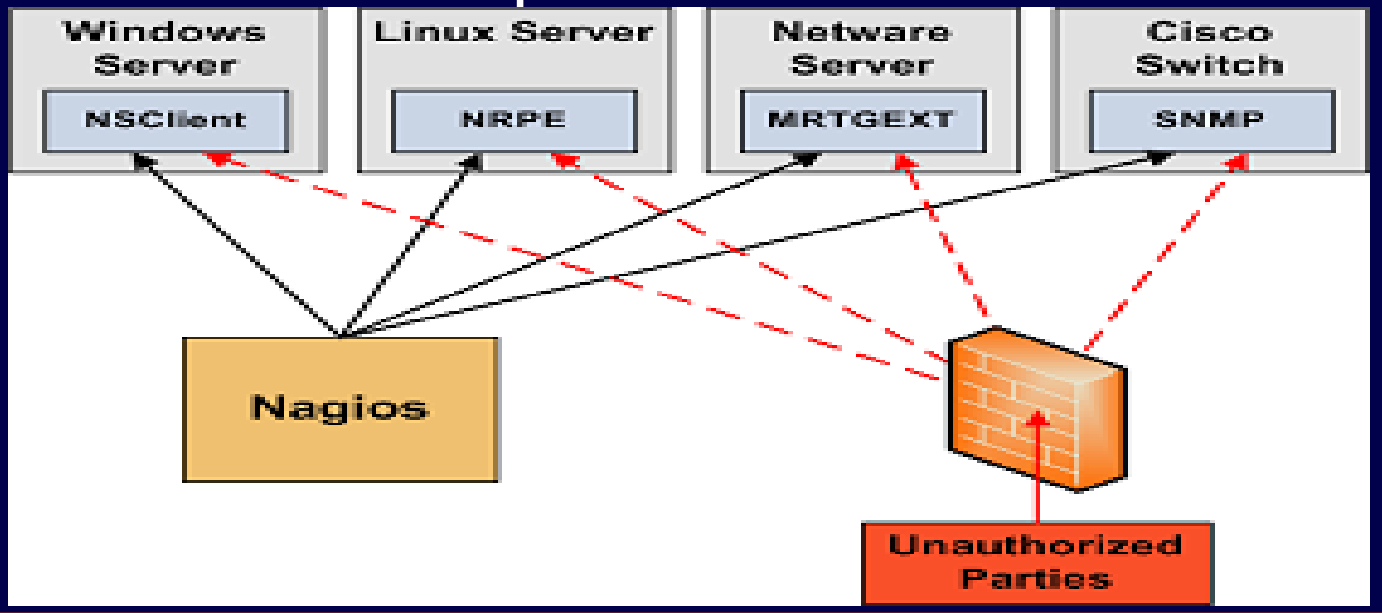
- Vaikimisi saab kirjutada vaid nagios ja veebiserveri kasutaja (apache) käsu failidesse.
- CGI-põhine veebirakendusel on võimalik seada kasutajanime ja parooli põhise autnentimisega juurdepääs.

Nagiose turvalisus IV

- Turvalisuse tõstmiseks tuleb kasutada skriptide koostamisel absoluutset rada (path).
- Makrode kasutamine võimaldab kasutajanimesid ja paroole hoida eraldi failis, mis pole veebiliidesele kätte saadavad ja veebiliidesele kätte saadavates failides kasutatakse muutujaid näiteks $USERn$.

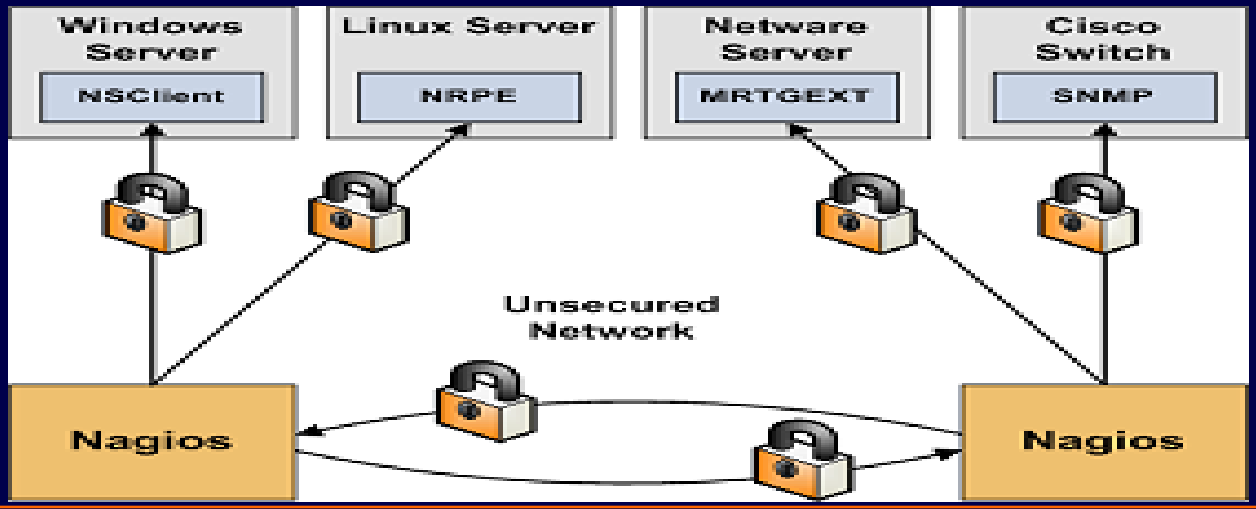
Nagiose turvalisus V

- Makrode koostamisel ei tohi kasutada tähemärke, mida shelli skript võib vääralt interpreteerida.

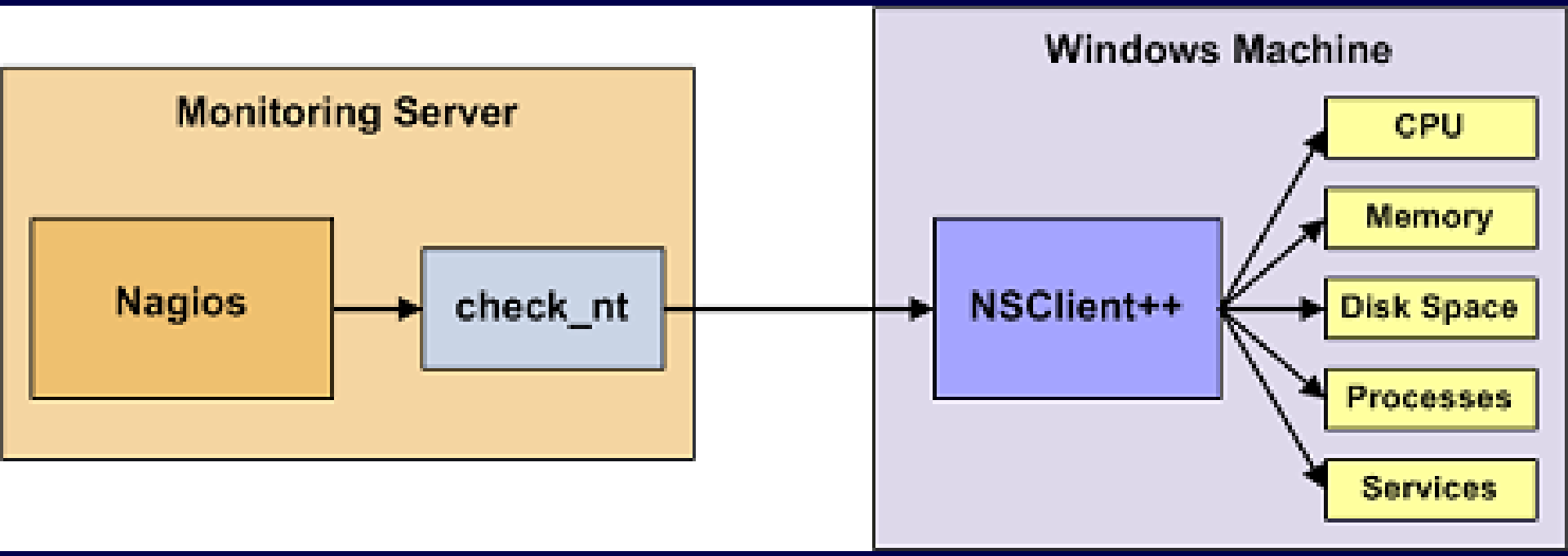


Nagiose turvalisus VI

- Nagioses on võimalus krüpteerida suhtlemine seireserveri ja väliste pluginate, moodulite vahel, nagu NSClient, NRPE või SNMP.

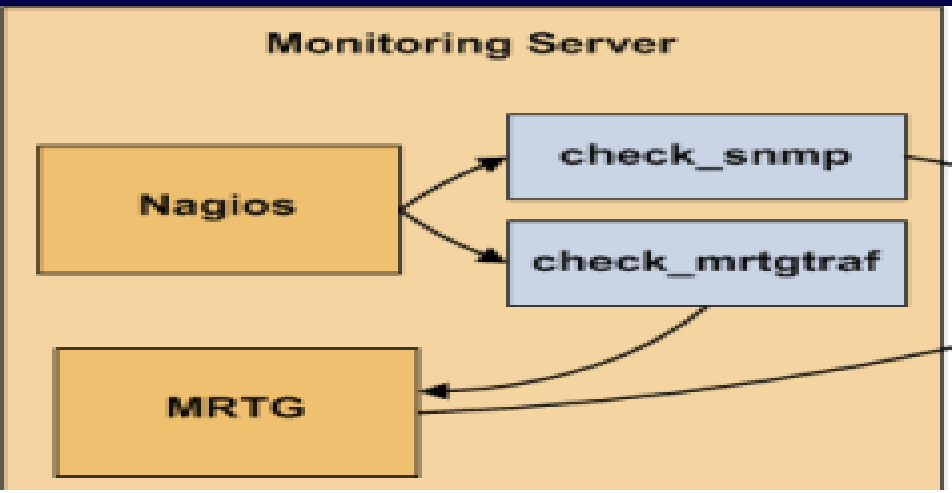


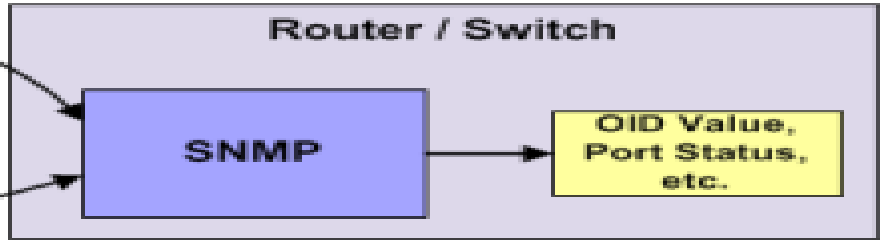
NSClient++ moodul MS Windows masinate seireks

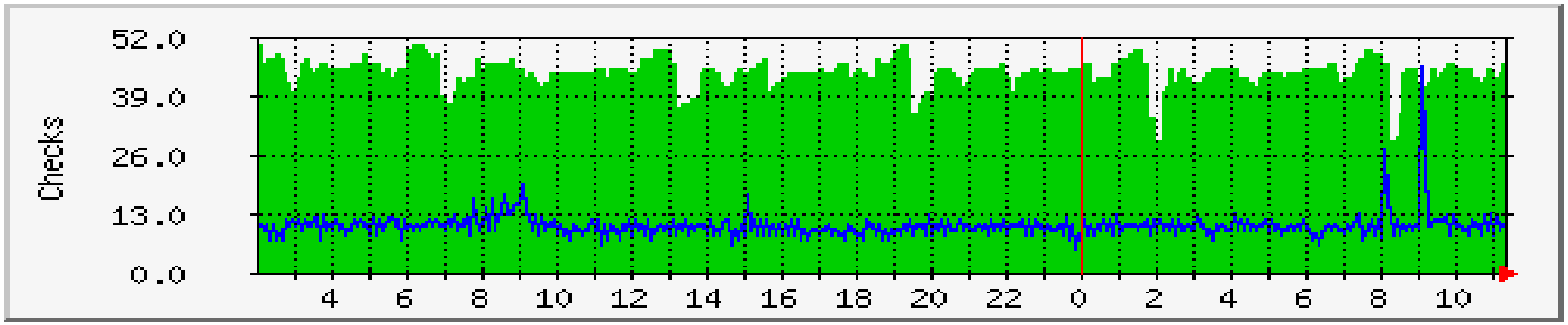


- NSClient++ töötab seiratavas arvutis
- Aktiivseire, VPN vajalik (avalik võrk)

MRTG graafikud Nagioses

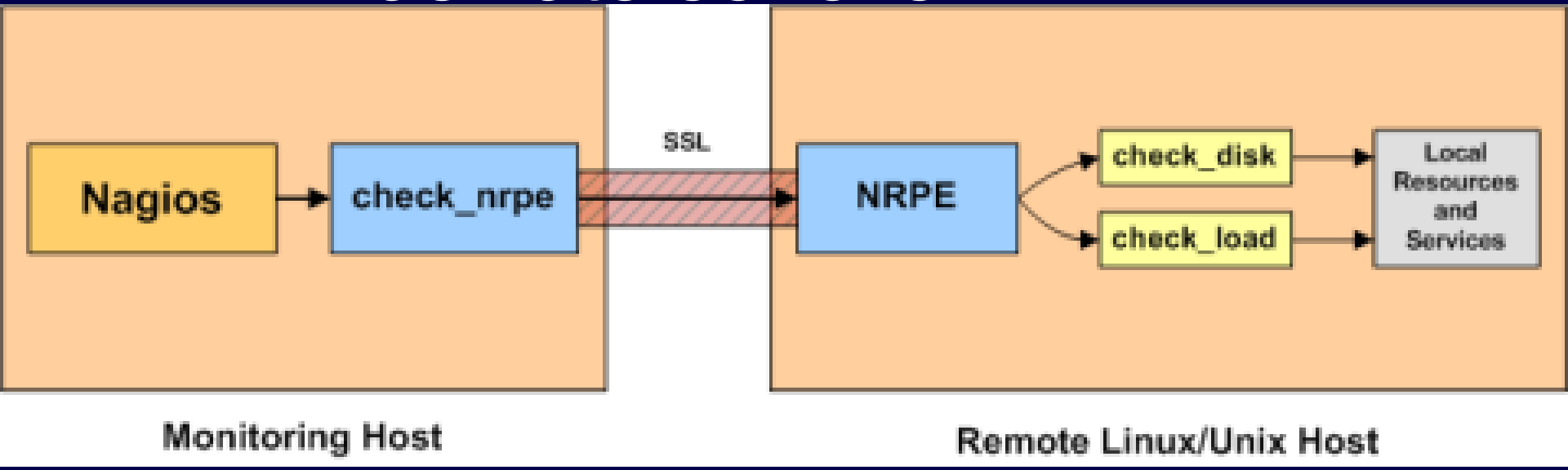






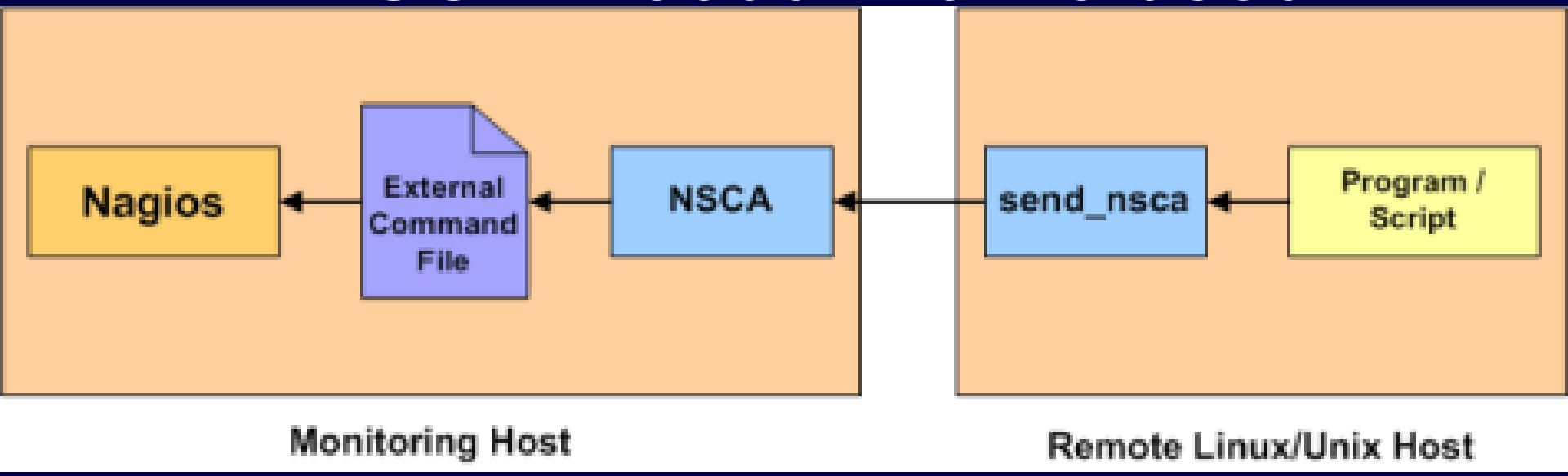
Max Scheduled Checks: 50.0 Average Scheduled Checks: 44.0 Current Scheduled Checks: 46.0
Max On-Demand Checks: 45.0 Average On-Demand Checks: 10.0 Current On-Demand Checks: 10.0

NRPE moodul UNIX/Linux masinate seireks



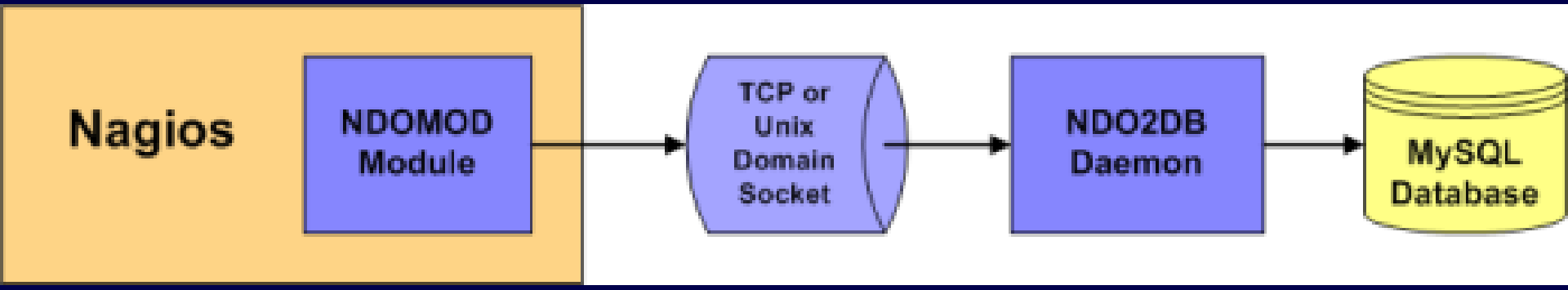
- NRPE moodul töötab seiratavas arvutis
- Avaliku võrgu korral VPN tunnal vajalik
- Tegemist on aktiivse seirega

NSCA mooduli võimalused



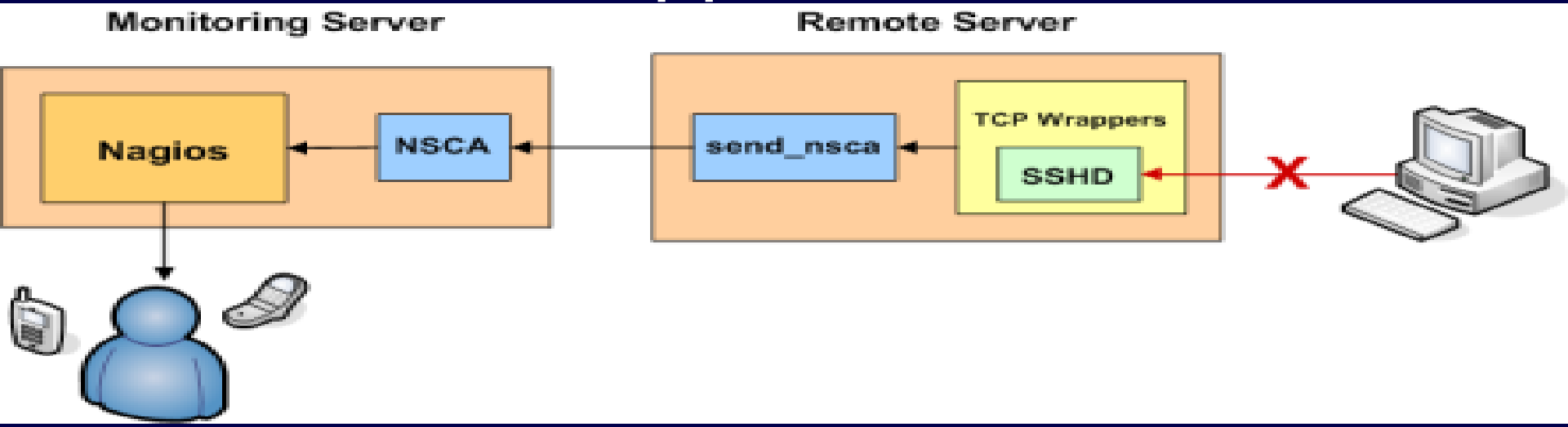
- Passiivne seirerežiim
- Teateid saadab kaugarvuti
- Võimaldab teadete krüpteerimist
- Sobib liias-, hajusseire lahendustesse

NDOUtils mooduli võimalused



- Võimaldab logid salvestada andmebaasi.
- Võimaldab CGI-põhise veebiliidese asendada PHP-põhise veebiliidesega.
- Nagiose tulevased lahendused hakkavadki hoidma logide andmeid MySQL andmebaasis.

TCP Wrapper moodul



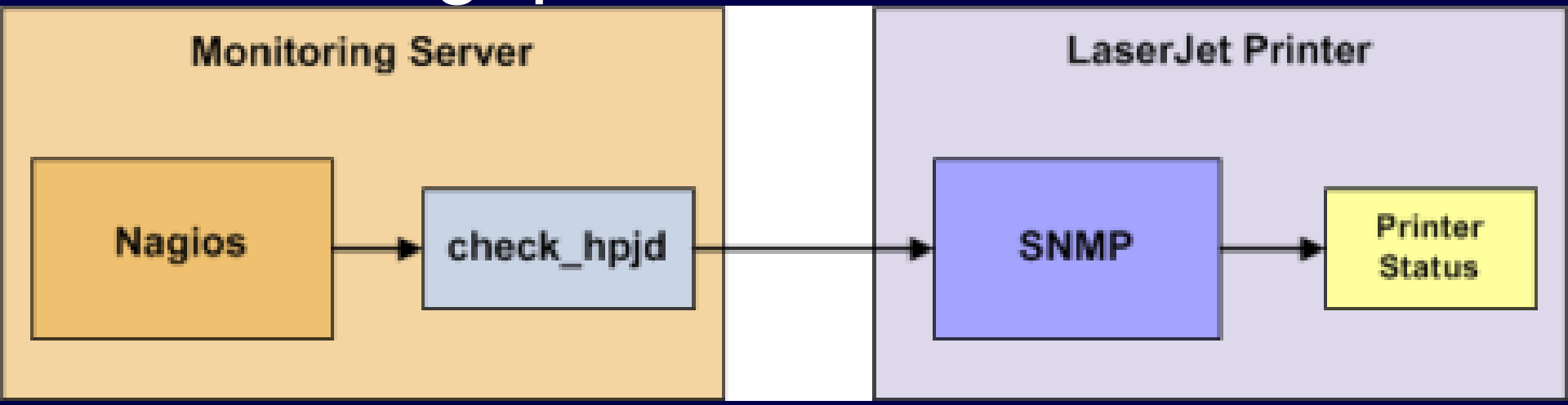
- Võimaldab genereerida alarmteateid, mitte lubatud aadressilt soovitakse SSH serverisse ühendus luua.
- Joonis kirjeldab kogu protsessi ja kasutusel on NSCA moodul, seega tegemist on passiivseirega.
- Antud andmeside sisaldab vahendeid edastatavate teadete krüpteerimiseks.
- Antud lahendus on efektiivne avastamaks portide skaneerimist.

SNMP ja SNMP Trap teenused Nagioses

Nagios:

- ei asenda täis SNMP haldusrakendust. Näiteks HP OpenView või OpenNMS.
- võimaldab SNMP Trap teate saabudes genereerida erinevaid vastuseid.
- SNMP Trap seire on passiivrežiimis.
- „Alex Burger's SNMP Trap Translator“ projekt, mis teeb Nagiosele SNMP Trapi arusaadavaks.
- Nagios oskab kasutada ka SNMP protokolli, selleks tuleb paigaldada Net.SNMP või SNMPTT moodulid.

Võrguprinterite seire



Eeldus

- JetDirect-liidese olemasolu printeril (JetDirect protokoll)
- SNMP liidese olemasolu printeril (SNMP sisse lülitatud)

Saab seirata järgnevaid sündmusi:

- Paper Jam, Out of Paper, Output Tray is Full
- Printer Offline, Toner Low, Insufficient Memory
- Open Door, Intervention Required

Nagiosega seotud veebilehti

- Nagios Plugins
- Nagios Community
- NagiosExchange
- Nagios On CD – Nagiose LiveCD
- Nagiose 3D kaardi programmid (VRML)
- Nagiose 2D ja 3D kaardi seadistamine
- Nagiose kohta info Wikipedias

Küsimused?