Choosing Plugins

Mike Weber

mweber@spidertools.com

Identifying Options

- Public Port Monitoring
- NRPE - Nagios Remote Plugin Executor
- SSH - Secure Shell
- NSClient++
- NSCA - Nagios Service Check Acceptor
- NRDP - Nagios Remote Data Processor
- SNMP - Simple Network Monitoring Protocol

Criteria for Selection

- ## Ease of Set Up
  How much time and effort to get it working?
- ## Network Topology
  Firewall – Is there a firewall between Nagios and Client?
  Internet – Does the check have to go over a public network?
  Internal Network/VPN – Is it on a secure network?
- ## Security
  Security for Nagios
  Security for Client
- ## Resource Usage
  Total RAM usage on client and server
  Total CPU usage on client and server
  Total Time usage on client and server

Principles: Nagios Efficiencies in Scale

- Poor choices on implementing plugins cannot be compensated for by additional hardware.
- If possible, execute plugins on the client using either SSH, NRPE, NSCA, NRDP.
- Compiled plugins require 10 - 44 times LESS resources than scripts.
- (Plugin RAM + Nagios RAM) x Time = RAM per check
- Plugins hold resources for up to 10 seconds.

Ease of Set Up

Nagios®
World Conference
North America

Ease of Set Up - Order

- Public Port Monitoring
- NRPE
- NSClient++
- SSH
- NRDP
- NSCA
- SNMP

Ease of Set Up – Public Ports

- Advantages

  Can be set up with no client modification.
  No firewall issues (the nature of public access).

- Disadvantages

  Limited external port information.
  Plain text transfer of usernames/passwords if monitoring accounts.
  Limited internal access information (processes, resources, etc.)

Ease of Set Up – NRPE

- Advantages

  Complete access to internal and external aspects (plugins and scripts).

- Disadvantages

  Must set up an agent or daemon on the client.
  Data transferred plain text (typical installation).

Ease of Set Up – NSClient++

Advantages

Complete access to internal and external aspects (plugins and scripts).
Use NRPE, check_nt or other options and programming languages.
Password authentication available.

Disadvantages

Must set up an agent or daemon on the client.
Password authentication method weak.
Data transferred plain text (typical installation).

Ease of Set Up – SSH

Advantages

Complete access to internal and external aspects (plugins and scripts).
Secure connection and secure data transfer.

Disadvantages

Must set up keys for nagios user.
Requires modification of firewall and/or tcp_wrappers.
May require sudo permissions (set up with visudo).

Ease of Set Up – NRDP

Advantages

Complete access to internal and external aspects (plugins and scripts).
Password authentication.
Uses port 80 or 443 so no firewall issues.
No daemon to set up on Nagios.

Disadvantages

Requires the creation of a script on the client to send data.
No encryption unless you use SSL.

Ease of Set Up – NSCA

Advantages

Complete access to internal and external aspects (plugins and scripts).
Password authentication and encryption.

Disadvantages

Requires the creation of a script on the client to send data.
Requires the set up of the NSCA daemon on the Nagios server.
Must configure firewall and tcp_wrappers on the Nagios server.

Ease of Set Up – SNMP

- Advantages

  Flexible options for monitoring hardware.

- Disadvantages

  Requires knowledge of how SNMP works.
  Requires the set up of the SNMP daemon on the client or device.
  The snmpd.conf on the client requires at least 4 changes for accesss.

Network Topology

Nagios®
World Conference
North America

Network Typology

- Internal Network or VPN
  Perimeter firewall or VPN protects all communication.
- Public Network or Internet
  Attempts to compromise the system exist.
  Some protocols may be less reliable (UDP).
- Firewalls or Gateways
  Firewalls/Gateways must be modified to allow access.
  Firewalls/Gateways cannot be modified to allow access.

Network Typology – Internal Network

- ALL Options will work

  Public Ports
  NRPE
  NSClient++
  SSH
  NRDP
  NSCA
  SNMP

Network Typology – Public Network

- Secure Options Recommended

  Public Ports – no firewall configuration necessary
  SSH - SSH port can usually be opened or is open
  NSCA – passive scripts will work behind firewall
  NRDP – passive scripts will work behind firewall

- Extensive Security for Nagios Server

  Firewall limiting access to clients only.
  tcp_wrappers limiting access to clients only.
  Encrypted connections for administrators.
  ModSecurity to filter port 80/443 access (application firewall).

Security

Nagios®
World Conference
North America

Security Factors

- **Security on Nagios**
  Factors that either elevate or degrade security on the Nagios server.
- **Security on the Client**
  Factors that either elevate or degrade security on the client.
- **Security of Network Communication**
  Is the data transfer encrypted?
  Is the transfer protected by a password or token?

Security - SSH

Advantages

Data transfer is encrypted.
Login is encrypted.

Disadvantages

Security complexity – users, keys, connections, rights
Typically key uses empty password.

ssh-keygen -b 1024 -f id_dsa -t dsa -N ''

Use of visudo required to provide nagios user access to files and applications.

nagios ALL=NOPASSWD: /usr/local/nagios/libexec/check_init_service

Security - NSCA

- Advantages

  Choice on encryption methods.
  Password authentication.

- Disadvantages

  Complexity of setup – daemon,two config files to edit, password,encryption,firewall, tcp_wrappers, edit nagios.cfg

Security - NRDP

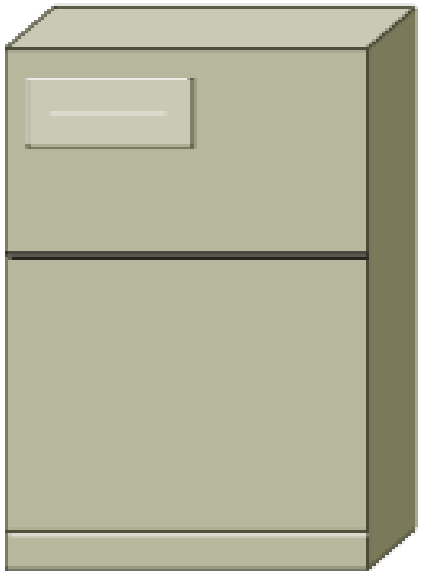
- Advantages

  Token used to secure connectivity.
  Uses port 80 so no new port must be opened.
  Could use port 443 so encrypted.

- Disadvantages

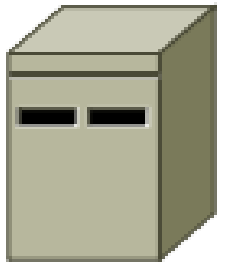
  Need to create script on client to collect data and send data to Nagios server.

Security - NRDP

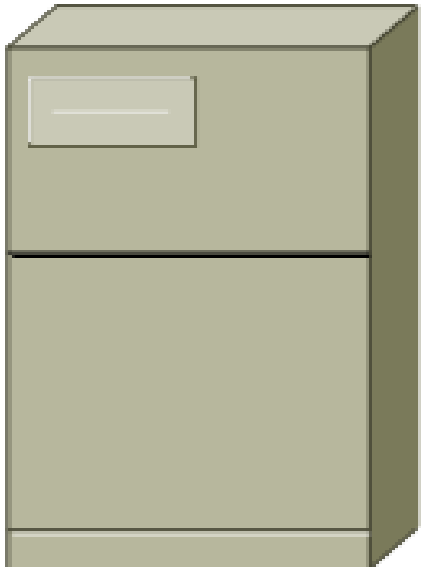


Nagios
Receive on 5667
NSCA Daemon
External Command

NSCA

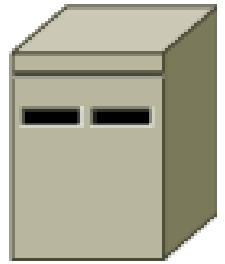


Security: password, encryption level



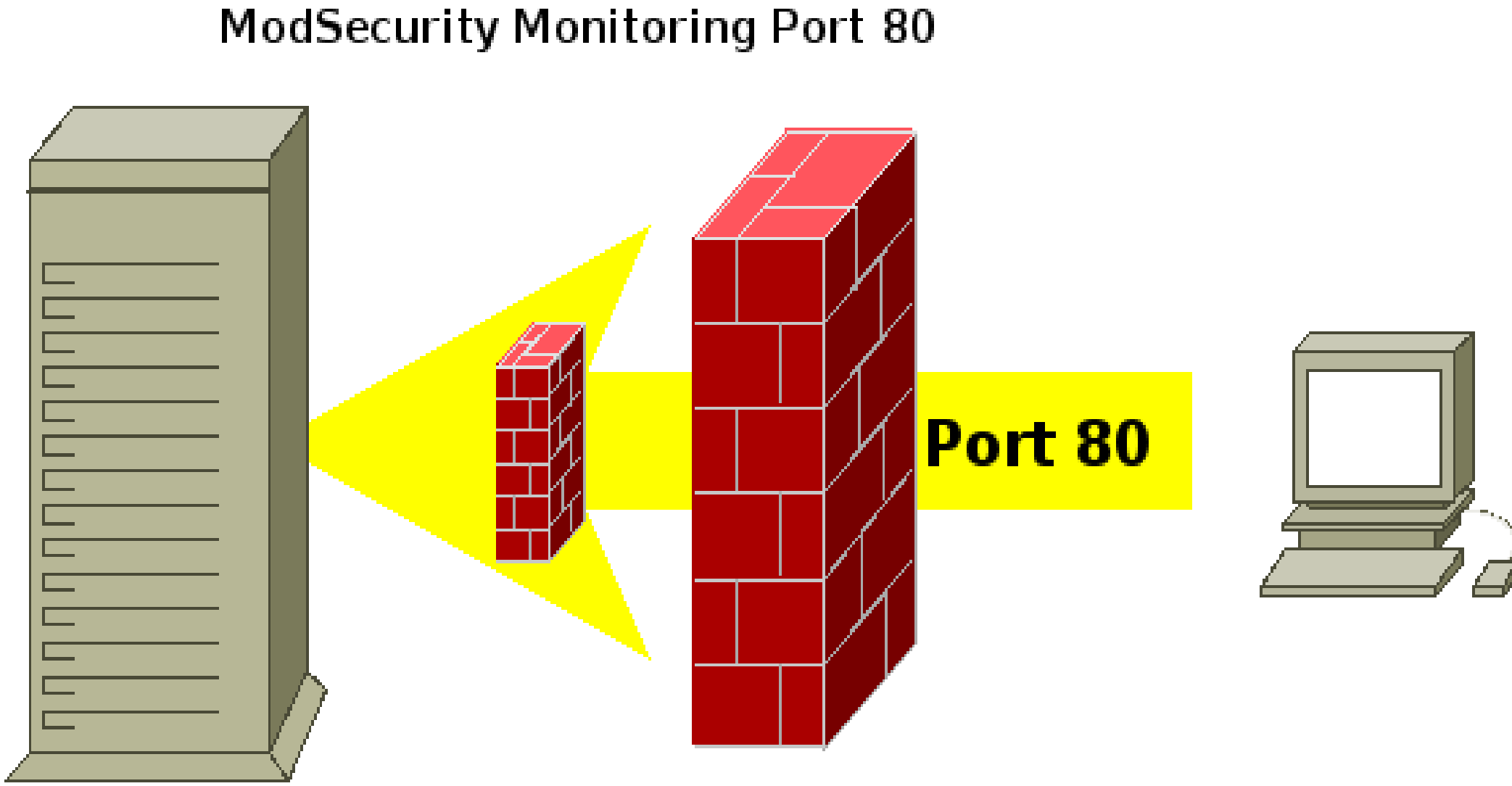
Nagios
Receive on 80 or 443
No Daemon
Sent to Core spool

NRDP



Security: token, 443 to web

Security – Web Interface



Resource Usage

Nagios®
World Conference
North America

Resource Usage

- Resources Used on Nagios
  Total RAM usage on server.
  Total CPU usage on server.
  Total Time usage on server.
- Resources Used on the Client
  Total RAM usage on client.
  Total CPU usage on client.
  Total Time usage on client.

Resource Usage

Nagios Server Resources

Operating System: Resources
* Base System
* syslog
* cron
* SSH
* sendmail/postfix

Support for Nagios:Resouces
* MySQL
* Postgres
* Apache

Nagios Plugins: Resources
* plugin
* Nagios connection

Resource Usage: Script to Capture Data

```
#!/bin/bash
i=0
until [ $i -eq 300 ]
do
        ps axo pid,ppid,pcpu,size,etime,priority,cmd | grep -v awk | grep -v bash |awk '/nagios/ {print}' >> nagios.txt
        ps axo pid,ppid,pcpu,size,etime,cmd | grep nagios |grep -v grep | grep -v nagios_total.sh |awk -f awk >> nagios.txt
        echo "# # # # # # # # #" >> nagios.txt
        sleep 1
        i=$(( $i +1 ))
done
echo "##### Nagios Process Report #####" >> nagios_summary.txt
echo "#####################################" >> nagios_summary.txt
echo "##### Total Memory Summary  #####" >> nagios_summary.txt
grep "Total Memory" nagios.txt | sort | uniq -c >> nagios_summary.txt
echo "##### Average Memory Use MB   #####" >> nagios_summary.txt
awk  '{ SUM += $4} END { print SUM/300/1024 }' nagios.txt >> nagios_summary.txt
echo                                  >> nagios_summary.txt
echo "#####################################" >> nagios_summary.txt
echo "#####  Total CPU Summary %  #####" >> nagios_summary.txt
grep "Total CPU" nagios.txt | sort -n | uniq -c >> nagios_summary.txt
grep "Total CPU" nagios.txt |awk '{printf "%3.2f\n", $3}'| sort -n > /tmp/nagios_summary
echo "#####    Average CPU Use    #####" >> nagios_summary.txt
awk  '{ SUM += $1} END { print SUM/300 }' /tmp/nagios_summary >> nagios_summary.txt
echo "#####    Maximum CPU Use    #####" >> nagios_summary.txt
sort -n /tmp/nagios_summary |tail -n1 >> nagios_summary.txt
```

Resource Usage - Compiled

PID	PPID	CPU	RAM	Time	PR	Command
32135	32134	0.0	356	00:01	15	/usr/local/nagios/libexec/**check_http** -H 192.168.5.1 -u /blog/ -s Nagios Test Page
32566	32564	0.0	356	00:01	21	/usr/local/nagios/libexec/**check_http** -H 192.168.5.1 -p 8080 -w 3 -c 7
32379	32378	0.0	340	00:02	25	/usr/local/nagios/libexec/**check_ftp** -H 192.168.5.1 -t 4 -e vsFTPd 2.0.5
31819	31818	0.0	280	00:24	25	/usr/local/nagios/libexec/**check_ping** -H 69.58.181.89 -w 3000.0,80% -c 5000.0,100% -p 5
32365	32364	0.0	280	00:02	18	/usr/local/nagios/libexec/**check_ping** -H 192.168.5.191 -w 3000.0,80% -c 5000.0,100% -p 5
32535	32534	0.0	1004	00:01	18	/usr/local/nagios/libexec/**check_nrpe** -H 192.168.5.191 -c check_cpu_stats
1633	1632	0.0	1004	00:01	18	/usr/local/nagios/libexec/**check_nrpe** -H 192.168.5.191 -c check_yum
1386	1385	0.0	340	00:02	20	/usr/local/nagios/libexec/**check_tcp** -H 192.168.5.1 -p 22
3209	3208	0.0	340	00:00	21	/usr/local/nagios/libexec/**check_tcp** -H 192.168.5.1 -p 993
3387	3386	0.0	340	00:00	15	/usr/local/nagios/libexec/**check_tcp** -H 192.168.5.1 -p 3306

Resource Usage – Compiled

PID PPID CPU RAM Time PR Command

1944 1943 0.0 504 00:01 18 /usr/local/nagios/libexec/**check_mysql** -H 192.168.5.1 -u nagios -d nagios --password XXXXXX

32558 32557 0.0 272 00:00 19 /usr/local/nagios/libexec/**check_by_ssh** -H 192.168.5.190 -i /usr/local/nagios/etc/.ssh/id_dsa -C /usr/local/nagios/libexec/check_load -w 5.0,4.0,3.0 -c 10.0,6.0,4.0

7979 7978 0.0 272 00:01 23 /usr/local/nagios/libexec/**check_by_ssh** -H 192.168.5.190 -i /usr/local/nagios/etc/.ssh/id_dsa -C /usr/local/nagios/libexec/check_net -w -c

3117 3116 0.0 272 00:01 16 /usr/local/nagios/libexec/**check_by_ssh** -H 192.168.5.190 -i /usr/local/nagios/etc/.ssh/id_dsa -C /usr/local/nagios/libexec/check_multi -f /usr/local/nagios/etc/check_multi/check_multi.cmd

32151 32150 0.0 256 00:01 15 /usr/local/nagios/libexec/**check_snmp** -H 192.168.5.220 -C public -m DISMAN-EVENT-MIB -o . 1.3.6.1.2.1.1.3.0

Resource Usage - Perl

PID PPID CPU RAM Time PR Command

31797 31796 1.0 5452 00:09 16 /usr/bin/perl -w /usr/local/nagios/libexec/**check_snmp_load.pl** -H 192.168.5.1 -C public -w 90% -c 95%

32031 32030 1.1 5320 00:08 15 /usr/bin/perl -w /usr/local/nagios/libexec/**check_snmp_mem.pl** -H 192.168.5.14 -C public -w 85,10 -c 95,20

32257 32254 4.0 5448 00:02 21 /usr/bin/perl -w /usr/local/nagios/libexec/**check_snmp_storage.pl** -H 192.168.5.1 -C public -m /home -w 95 -c 97 -f

1558 1557 10.0 5984 00:01 21 /usr/bin/perl -w /usr/local/nagios/libexec/**check_snmp_int.pl** -H 192.168.5.1 -C public -n eth0 -w 200,400 -c 0,600

1330 1329 0.0 4864 00:00 17 perl /usr/local/nagios/libexec/**check_imap_receive** -H 192.168.5.191 --username tom --password linux23 -s SUBJECT -s New York --capture-max Sales --nodownload --nodelete --ssl

32390 32389 5.5 6236 00:02 25 /usr/bin/perl /usr/local/nagios/libexec/**check_interface_table.pl** -H 192.168.5.220 -C -w -C

32432 32431 10.0 5844 00:01 20 /usr/bin/perl -w /usr/local/nagios/libexec/**check_ifstatus** -H 192.168.5.230 -C public -x 1

Resource Usage - NSClient++

PID	PPID	CPU	RAM	Time	PR	Command
32279	32278	0.0	280	00:00	15	/usr/local/nagios/libexec/**check_nt** -H 192.168.5.14 -p 12489 -v CPULOAD -l 5 80 90
32384	32383	0.0	280	00:01	25	/usr/local/nagios/libexec/**check_nt** -H 192.168.5.14 -p 12489 -v CLIENTVERSION
32480	32479	0.0	280	00:01	15	/usr/local/nagios/libexec/**check_nt** -H 192.168.5.14 -p 12489 -v UPTIME
1349	1348	0.0	280	00:00	18	/usr/local/nagios/libexec/**check_nt** -H 192.168.5.14 -p 12489 -v SERVICESTATE -d SHOWALL -l SNMP
1619	1618	0.0	280	00:01	15	/usr/local/nagios/libexec/**check_nt** -H 192.168.5.14 -p 12489 -v PROCSTATE -d SHOWALL -l Explorer.exe
1832	1831	0.0	280	00:00	22	/usr/local/nagios/libexec/**check_nt** -H 192.168.5.14 -p 12489 -v USEDDISKSPACE -l c -w 80 -c 90
3106	3105	0.0	280	00:02	17	/usr/local/nagios/libexec/**check_nt** -H 192.168.5.14 -p 12489 -v PROCSTATE -d SHOWFAIL -l Explorer.exe&Notepad.exe
32561	32560	0.0	332	00:01	21	/usr/local/nagios/libexec/**check_nrpe** -H 192.168.5.14 -c alias_service
1958	1957	0.0	332	00:02	16	/usr/local/nagios/libexec/**check_nrpe** -H 192.168.5.14 -c alias_disk
3205	3204	0.0	332	00:00	20	/usr/local/nagios/libexec/**check_nrpe** -H 192.168.5.14 -c alias_cpu
7838	7837	0.0	332	00:00	19	/usr/local/nagios/libexec/**check_nrpe** -H 192.168.5.14 -c alias_multiple

Resource Usage - SSH

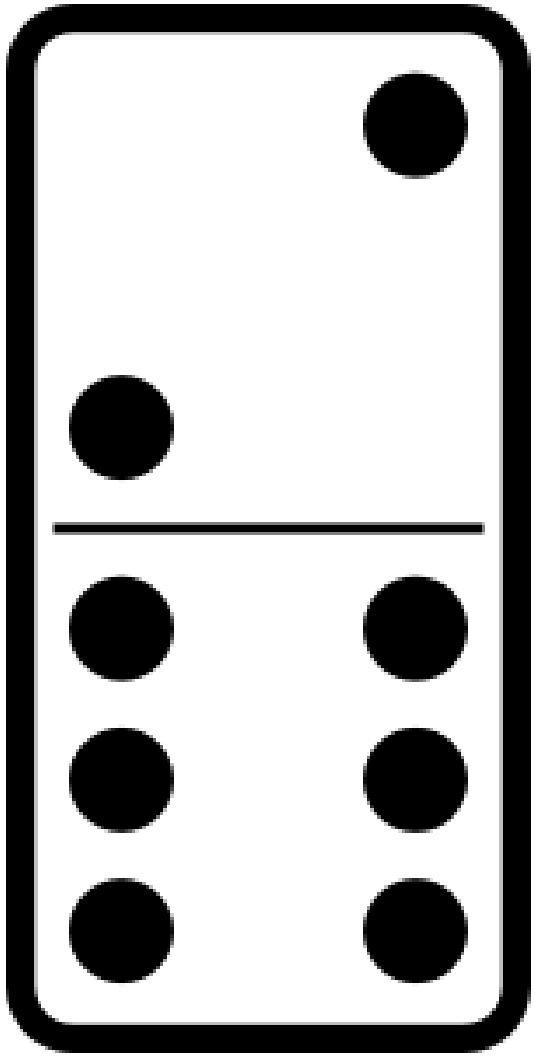
PID PPID CPU RAM Time PR Command

32562 32558 0.0 524 00:00 16 /usr/bin/**ssh** -i /usr/local/nagios/etc/.ssh/id_dsa 192.168.5.190 /usr/local/nagios/libexec/check_load -w 5.0,4.0,3.0 -c 10.0,6.0,4.0

5865 5860 0.0 524 00:01 15 /usr/bin/**ssh** -i /usr/local/nagios/etc/.ssh/id_dsa 192.168.5.190 /usr/local/nagios/libexec/check_dns -H nagios.org

3119 3117 0.0 524 00:01 15 /usr/bin/**ssh** -i /usr/local/nagios/etc/.ssh/id_dsa 192.168.5.190 /usr/local/nagios/libexec/check_multi -f /usr/local/nagios/etc/check_multi/check_multi.cmd

Principle #1: Poor choices on implementing plugins cannot be compensated for by additional hardware.



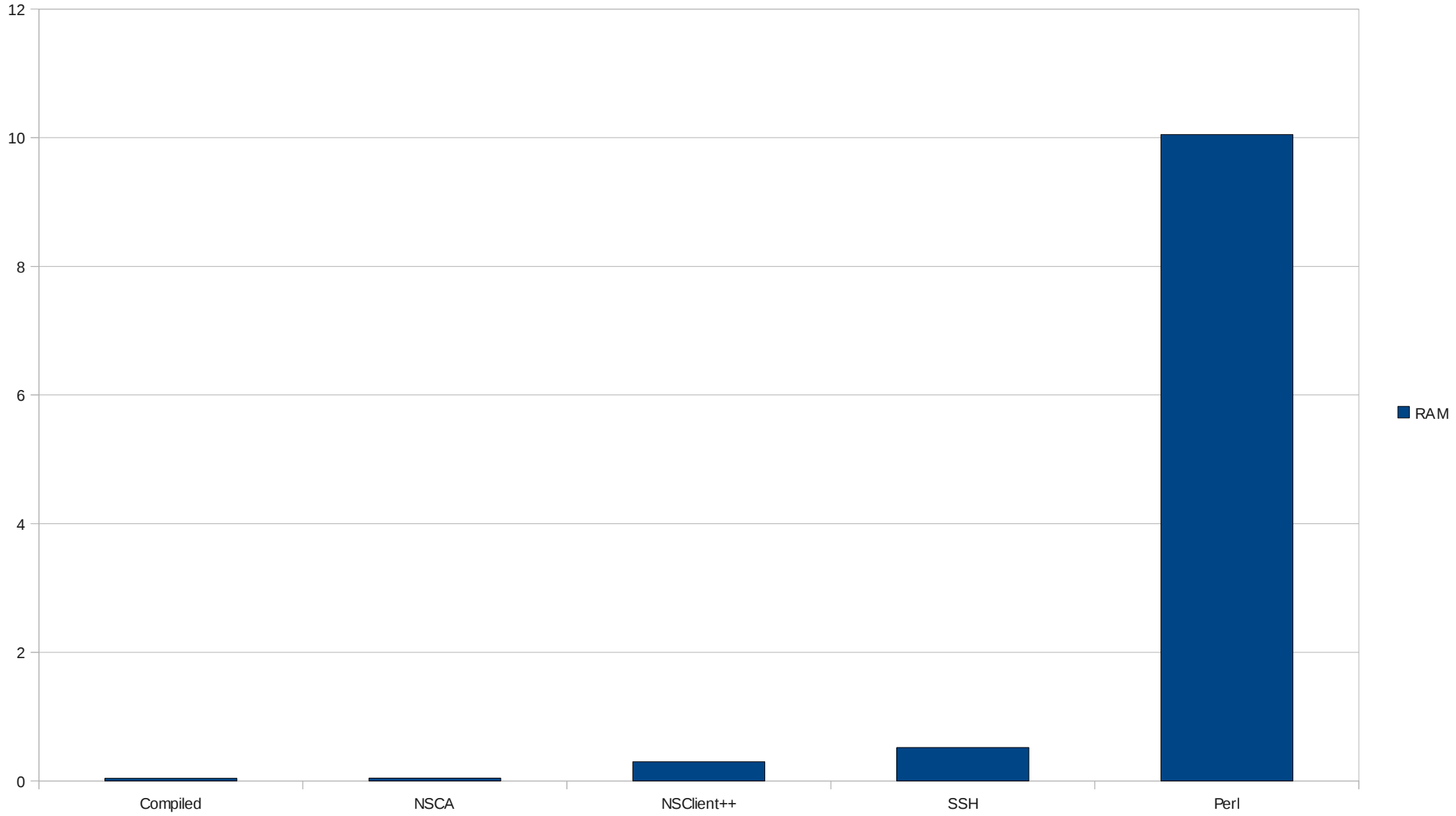
- Knowledge of Plugins
- Planning Saves
- Hardware Limits
- Avoid the Domino Effect

Principle #2: If possible, execute plugins on the client using either SSH, NRPE, NSCA, NRDP.

- Typical Client Under Utilized
- check_multi Most Efficient

  Collect 10-30 checks per connection
  Used with NRPE, SSH, NRDP, NSCA

Principle #3: Compiled plugins require 10 - 44 times LESS resources than scripts.

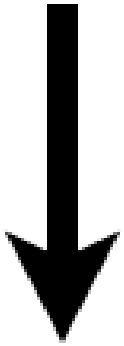


Principle #4: (Plugin RAM + Nagios RAM) x Time = RAM per check

- check_ping
  takes 280 RAM
  takes 10864 RAM from nagios process to execute plugin
  takes 3 seconds to execute
- (plugin RAM + nagios RAM) x time = RAM per check
- (280 +10864) X 3 = 32.64 MB RAM per check

RAM Required per Check

Nagios Process
Process ID = 11955
CPU = 0
RAM = 10864



Process Relationship

Total CPU to Perform Check = 0
Total RAM to Perform Check = 11144

Plugin - check_ping
Parent Process = nagios = 11955
CPU = 0
RAM = 280

Principle #5: Plugins hold resources for up to 10 seconds.

Example: check_ping

```
PID      PPID      CPU    RAM          Time              Command
12106   12105     0.0      280          00:01  25 /usr/local/nagios/libexec/check_ping -H
192.168.5.220 -w 3000.0,80% -c 5000.0,100% -p 5

12106   12105     0.0      280          00:02  25 /usr/local/nagios/libexec/check_ping -H
192.168.5.220 -w 3000.0,80% -c 5000.0,100% -p 5

12106   12105     0.0      280          00:03  25 /usr/local/nagios/libexec/check_ping -H
192.168.5.220 -w 3000.0,80% -c 5000.0,100% -p 5
```

Principle #5: Example

```
CPU   RAM        Time                          Plugin
13.0  7696       00:01  20 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 6.5  7696       00:02  20 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 4.3  7696       00:03  20 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 3.2  7696       00:04  20 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 2.6  7696       00:05  20 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 2.1  7696       00:06  15 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 1.8  7696       00:07  15 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 1.6  7696       00:08  15 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 1.4  7696       00:09  15 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
 1.3  7696       00:10  15 /usr/bin/perl -w? /usr/local/nagios/libexec/check_iftraffic3.pl
```