CS312 Solutions #4

March 9, 2015

Solutions

1. (1 pt) Describe three resources you might want to monitor on a server. Elaborate on how you might decide on acceptable thresholds for each resource.

   This answer can vary but some good resources to check include: server load, disk usage, memory, swap usage, services such as http and ssh, network traffic, and server pingable to name a few. The thresholds depend on the resource, however generally its a value that allows you to respond before the service goes completely down. You also need to consider rate of change sometimes because of things like logrotation.

2. (1 pt) Describe in detail the four components of Nagios.

   (a) **Core Server Process: Provides core logic for monitoring, keeps track of service states, and initiates service checks.**

   (b) **CGI Web Interface: Simple web interface which connects to the core server process via sockets.**

   (c) **Plugins: Scripts written to gather monitoring information. Typically written in Perl, but can be written in about anything. Has an API that you follow to create your own plugin.**

(d) **NRPE/NSCA Agents: Daemons that actually execute the plugin on a server. NRPE: Active checking daemon. NSCA: Passive checking daemon**

3. (1 pt) Name three primary differences between active checks vs. passive checks for monitoring.

   (a) **Active checks are initiated from a central server while passive checks are initated from the remote host.**

   (b) **Active checks require a daemon listening on a port to run on the remote server, while passive checks only require a daemon listening on a port on the central server.**

   (c) **Active requires a central server to schedule checks to the remote hosts.**

   (d) **Passive checks can scale much better than active checks.**

   (e) **Passive checks work behind a firewall easier than Active checks.**

4. (5 pt) Create a new openstack VM and complete the following tasks. Keep in mind you will need to reload the `nagios` service each time you change the configuration file.

   (a) Install nagios and all of the nagios plugins. Show the commands you used.

```
$ yum install epel-release
$ yum install nagios nagios-plugins*
```

   (b) Start and enable Apache, Nagios and NRPE daemons. Show the commands you used.

```
$ service httpd start
$ service nagios start
$ service nrpe start
$ chkconfig httpd on
$ chkconfig nagios on
$ chkconfig nrpe on
```

   (c) Go to the nagios page `http://<your ip>/nagios` and login using `nagiosadmin` for both the user and password. Click on `Services` under `Current Status`. Copy and paste what you see for `localhost` including its services.

```
localhost
Current Load
OK  03-05-2015 22:11:59 0d 0h 3m 26s  1/4 OK - load
    ↪ average: 0.01, 0.06, 0.02
Current Users
OK  03-05-2015 22:11:59 0d 0h 2m 48s  1/4 USERS OK - 1
    ↪ users currently logged in
HTTP
Notifications for this service have been disabled
WARNING 03-05-2015 22:12:59 0d 0h 2m 11s  3/4 HTTP
    ↪ WARNING: HTTP/1.1 403 Forbidden - 5152 bytes in
    ↪ 0.001 second response time
PING
OK  03-05-2015 22:11:59 0d 0h 1m 33s  1/4 PING OK -
    ↪ Packet loss = 0%, RTA = 0.06 ms
Root Partition
OK  03-05-2015 22:12:28 0d 0h 1m 25s  1/4 DISK OK -
    ↪ free space: / 8562 MB (89% inode=94%):
SSH
Notifications for this service have been disabled
OK  03-05-2015 22:13:06 0d 0h 1m 25s  1/4 SSH OK -
    ↪ OpenSSH_5.3 (protocol 2.0)
Swap Usage
OK  03-05-2015 22:11:59 0d 0h 1m 25s  1/4 SWAP OK -
    ↪ 100% free (511 MB out of 511 MB)
Total Processes
OK  03-05-2015 22:11:59 0d 0h 1m 25s  1/4 PROCS OK: 98
    ↪ processes with STATE = RSZDT
```

(d) Fix the HTTP check for the localhost object config (`/etc/nagios/objects/localhost.cfg`) so that it checks the `/nagios` URL. Make sure it returns OK (Hint: look at the help for the `check_http` plugin). Copy and paste the HTTP check on the nagios page. Also show the HTTP service definition including the changes you made to fix the check.

```
HTTP
OK  03-05-2015 22:18:09 0d 0h 0m 2s 1/4 HTTP OK: HTTP
    ↪ /1.1 301 Moved Permanently - 552 bytes in 0.001
    ↪ second response time
```

```
define service{
  use                     local-service
  host_name               localhost
```

```
  service_description   HTTP
  check_command         check_http!-u /nagios -a
     ↪ nagiosadmin:nagiosadmin
  notifications_enabled 0
}
```

(e) Using the same config file above, create a new host to check called `cs312-server` using the IP `140.211.15.183`. Add ping, ssh and an http check for `http://cs312.osuosl.org`. Show the config you used and paste the output from the nagios page for the host including its services. Show the config line(s) you changed.

```
define host {
  use       linux-server
  host_name cs312-server
  alias     cs312-server
  address   140.211.15.183
}

define service {
  use           local-service
  host_name     cs312-server
  service_description HTTP
  check_command check_http!-H cs312.osuosl.org
}

define service{
  use                 local-service
  host_name           localhost,cs312-server
  service_description PING
  check_command       check_ping!100.0,20%!500.0,60%
}

define service{
  use                   local-service
  host_name             localhost,cs312-server
  service_description   SSH
  check_command         check_ssh
  notifications_enabled 0
}
```

```
cs312-server
HTTP
OK  03-05-2015 22:41:04 0d 0h 1m 40s  1/4 HTTP OK: HTTP
   ↪ /1.1 200 OK - 9460 bytes in 0.002 second response
```

```
    ↪  time
PING
OK  03-05-2015 22:40:36 0d 0h 1m 40s  1/4 PING OK -
    ↪ Packet loss = 0%, RTA = 0.50 ms
SSH
OK  03-05-2015 22:41:36 0d 0h 1m 40s  1/4 SSH OK -
    ↪ OpenSSH_5.3 (protocol 2.0)
```

(f) Rename the `check_hda1` check in the NRPE config to `check_all_disks`. Fix the command so that it checks all of the disks.

```
command[check_all_disks]=/usr/lib64/nagios/plugins/
    ↪ check_disk -w 20% -c 10% -A
# OR
command[check_all_disks]=/usr/lib64/nagios/plugins/
    ↪ check_disk -w 20% -c 10%
```

(g) Extra Credit (2pts): Show the command you would use to manually check to see if the NRPE check is working on the localhost. Also show the output of the command.

```
$ /usr/lib64/nagios/plugins/check_nrpe -H 127.0.0.1 -c
    ↪ check_all_disks
DISK OK - free space: / 8560 MB (89% inode=94%); /dev/
    ↪ shm 245 MB (100% inode=99%);| /=974MB
    ↪ ;8036;9041;0;10046 /dev/shm=0MB;196;220;0;245
```

5. (1 pt) What is the difference between a recursive DNS server and an authoritative one? Explain when you would use each.

   (a) **A recursive DNS server is used to resolve answers for queries, typically originating from the same network. It will answer non-authoritatively, usually by querying the authoritative server and caching the answer.**

   (b) **An authoritative DNS server usually only answers for domains that it is authoritative for, and no others.**

   (c) **An authoritative server should be used when you are running a nameserver for your domain, and a recursive when you want DNS resolution for your machines.**

6. (1 pt) Please give a brief explanation of the following DNS record types:

```
A
AAAA
CNAME
MX
NS
NXDOMAIN
```

(a) **A - Translates a domain into an IPv4 address**

(b) **AAAA - Translates a domain into an IPv6 address**

(c) **CNAME - Translates a domain into another domain**

(d) **MX - Used to find mail servers for a domain**

(e) **NS - Used to find nameservers for a domain**

(f) **NXDOMAIN - Equivalent to no record found**

7. (1 pt) What is a glue record? Give a brief explanation of why they are necessary.

   A glue record is an A record held by the authoritative nameserver one node up the tree. It is necessary to solve the bootstrapping problem; it informs the client where to find a nameserver for a domain so that they don't have to ask that particular nameserver where it is.

8. (2 pt) What are specificity and sensitivity? Give a 1-2 sentence description of each.

   Specificity is the true-negative rate. In otherwords, it is the rate of true negatives compared to total reported negatives. Sensitivity is the true-positive rate, and is the ratio of true positives over total positives.

9. (1 pt) Give an example of a highly sensitive test that has low specificity.

   A highly sensitive test has a high true-positive rate. A test with low specificity has a high rate of false-negatives. In other words, the test correctly identifies positives but incorrectly

identifies negatives. Specific examples will vary.

10. (1 pt) What is time-series data? Give an explanation of why it is important.

    Time series data is a set of vectors consisting of a value and a timestamp. This data is important because it is a common format for displaying and analyzing metrics.

11. (2 pt) Why does DHCP use the broadcast routing scheme?

    Because DHCP involves getting the route and network, the machine cannot possibly know ahead of time who it should be talking to. Every device on the network listens to the broadcast address, so it is the only known way to reach the DHCP server before information is exchanged.

12. (3 pt) Name the three types of allocation DHCP servers can use. Give an explantion of each.
    (a) **Dynamic: The standard form of allocation**
    (b) **Automatic: Like Dynamic, but with permanent allocations**
    (c) **Static: Addresses are pre-allocated by MAC address**