



# Use Examples From the ccBay Pilot

## Diagnostic Questions Answered

**User:** network/system administrator who owns DNS

**Question:** The help desk says that some users can't resolve hosts in the CS domain but they can. What's wrong?

**Administrator:** *What errors are on the recursive DNS servers?*

```
$ccbay-query --query="ServerIP='192.168.68.17' and "ServerIP='192.168.68.13' and \  
WarnLevel='err'" -s -Ea -l30 | less
```

Displaying 30 of 582 events

```
2004-09-23 21:07:02.30:error:ns7.bigu.edu:192.168.68.17:lin-ulogd:
```

```
ProcessElement:named:3194:zone cs.bigu.edu/IN: refresh: failure trying master  
192.168.24.202#53: timed out
```

**Administrator:** *What errors are on the authoritative DNS server?*

```
$ccbay-query --query="ServerIP='192.168.8.202' and WarnLevel='err'" -s -Ea -l10 | less
```

Displaying 10 of 82 events

```
2004-09-23 21:33:17.20:error:ans.bigu.edu:192.168.8.202:lin-ulogd:
```

```
ProcessElement:named:3194:updating zone 'cs.bigu.edu/IN': update failed:  
'RRset exists (value dependent)' prerequisite not satisfied (NXRRSET)
```

**Administrator:** *Problem found, authoritative name server accidentally removed from zone file.*

**User:** developer (ccBay)

**Question:** I can verify that the web application on e2ed1.andrew.cmu.edu was having problems around noon when I installed a new version of the application. What is the problem?

**Administrator:** *What errors are occurring in the web logs on e2ed1.andrew.cmu.edu?*

```
$ccbay-query --query="ServerIP='128.2.6.48' and WarnLevel='err' and ProcessName='httpd' \  
and TimeStart>'2004-09-23:11:5500.00'" -s -Ea
```

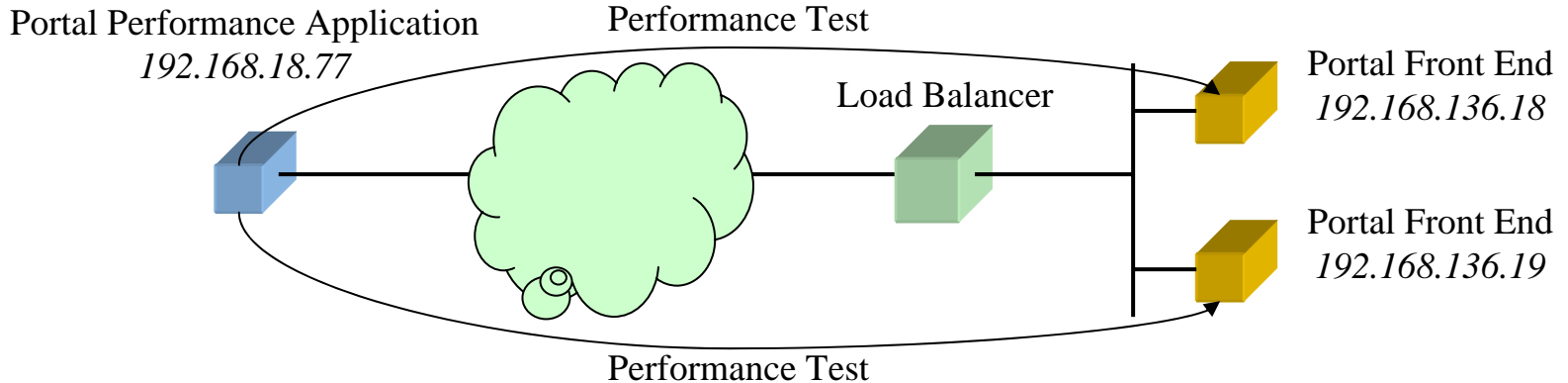
```
2004-09-23 19:01:00.00:err:e2ed1.andrew.cmu.edu:128.2.6.48:apached:ProcessElement:  
httpd:None:Client IP: 67.127.171.89 Message: File does not exist:  
/usr/www/htdocs/scripts/showresults.py?id=4xcF34Df
```

**Administrator:** *Problem found, wrong file name and path in application.*

# Application/Performance Related (future)

**User:** GRID/system administrator owner of a portal

**Question:** Users are complaining that the portal much slower today, is it?



# Application Related (future)

**User:** GRID/system administrator owner of a portal

**Question:** Users are complaining that the portal much slower today, is it?

**Administrator:** *What operation is taking longer then normal on front end server 192.168.136.18?*

```
$ccbay-query --query="ServerIP='192.168.18.77' and WarnLevel='info' and  
Target='192.168..136.18'" -s -Ep -l30 | less
```

Displaying 30 of 582 events

```
2004-09-23 21:07:02.30:info:portal0.bigu.edu:192.168.136.18:lin-perflogd:
```

```
ProcessElement:portperfcheck:3014:GET:/:resp=2.0sec;POST:/cgi-bin/perfcheck?  
user=test&pass=foo&test=quickperf:total=10.2sec,registration=3.4sec,dbtest=5.6
```

**Administrator:** *What operation is taking longer then normal on front end server 192.168.136.19?*

```
$ccbay-query --query="ServerIP='192.168.18.77' and WarnLevel='info' and  
Target='192.168..136.19'" -s -Ep -l30 | less
```

Displaying 30 of 582 events

```
2004-09-23 21:07:02.30:info:portal1.bigu.edu:192.168.136.19:lin-perflogd:
```

```
ProcessElement:portperfcheck:3014:GET:/:resp=4.2sec;POST:/cgi-bin/perfcheck?  
user=test&pass=foo&test=quickperf:total=26.8sec,registration=13.4sec,dbtest=11.6sec
```

**Administrator:** *Need to take 216.91.136.19 out of load balancer pool and examine further.*

**User:** network/system administrator

**Question:** The help desk says that some users can use the portal while others cannot? What is the problem?

**Administrator:** *Are the hosts that can't use the web service getting to the firewall?*

```
$ccbay-query --query="SourceIP='10.2.24.44' and 'DestinationIP='192.168.24.84' and \  
DestPort='80' ServerIP='192.168.2.45'" -s -En | less  
2004-09-23 17:18:14.00:2004-09-2300:00:00.00:info:outsidefw.bigu.edu:192.168.168.13:  
netflowd:NetworkElement:10.2.24.44:192.168.24.84:N/A:6:564:3332:  
80:6 (TCP):Active=0.551 ms; BytesPerPacket=94; Flags=0x1b
```

^c

**Administrator:** *Since we're getting to the firewall, are we getting through to the other side?*

```
$ccbay-query --query="SourceIP='10.2.24.44' and 'DestinationIP='192.168.24.84' and \  
DestPort='80' and ServerIP='192.168.2.24'" -s -En -l24
```

Displaying 0 of 0 events

\$

**Administrator:** *Problem found on firewall/, incorrect netmask.*

**User:** engineering manager of a web services group

**Question:** Are there malicious http requests being sent to any of my Web servers?

**Answer:** The manager requests a count of the events originating from Snort that are Web server related alerts.

```
$ ccbay-query -q "CollectorName='snortd' and ReferenceSystem like '%WEB%'" | wc  
38 837 14304
```

If 'wc' shows a line count other than 0, these Snort alerts need to be investigated with further queries to verify that the Web server accessed returned a status value other than 200 (success). To determine which exploits were attempted, the query above is run again, this time without the 'wc' redirection (next slide)...

# Security Related

**User:** engineering manager of a web services group

**Question:** What are the malicious http requests being sent to my Web servers?

**Answer:** The manager requests all events originating from Snort that are Web server related alerts.

```
$ ccbay-query -q "CollectorName='snortd' and ReferenceSystem like '%WEB%'"
```

```
<snip>
```

```
2004-09-24
```

```
02:07:27.00:alert:cmu6:192.168.2.7:snortd:SecurityElement:24.60.136.78:66.33.216.70:N/A:0:0:32767:
```

```
80:TCP:[1:1149:12] WEB-CGI count.cgi access:0:ID: Snort Version 2.2.0RC1 (Build 28)
```

```
Classification: access to a potentially vulnerable web application Priority: 2
```

```
<snip>
```

The manager is shown a detailed list of the Snort Web server related alerts. One of them is displayed here. The manager now needs to verify that none of his Web servers successfully responded to the Web request for this page or any of the other malicious http requests reported by Snort (next slide)...

**User:** engineering manager of a web services group

**Question:** Were any of the malicious http requests reported by Snort successfully replied to?

**Answer:** The manager verifies that all malicious page requests are treated as HTTP errors.

```
$ ccbay-query -q "CollectorName='apached' and EventMessage like 'Status: 200' and EventMessage like 'count.cgi'"  
$
```

The query above asks for all Apache events for the suspected malicious page that resulted in a successful status of 200. In this case, the query application does not display any matching events. This indicates that the Web server did not respond to this request and generated a 404 status or other error value instead.