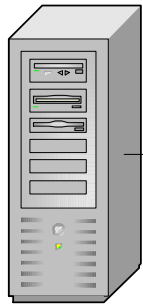


Boston Regional Domain

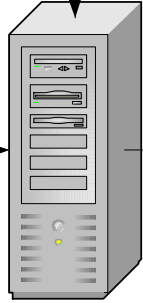
Waban Branch Domain

Newton Branch Domain



cmu1
10.54.2.2/24
Fedora Core 2

*Normalizing/
Forwarding Agents:*
lin-hlogd
lin-ulogd
sysevt



cmu2
10.54.2.3/24
Fedora Core 2

*Normalizing/
Forwarding Agents:*
apached
sysevt

Storage Agent:
ccBay-sqlize

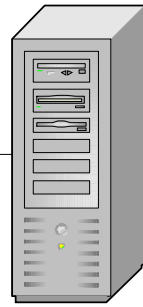
Storage/Forwarding Agent:
storforwd

Application Agents:
ccBay-query
ccBay-webconsole
lin-xmlevt



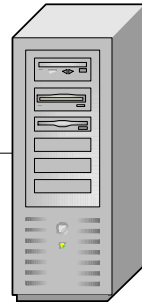
cmu3
10.54.2.4/24
Red Hat 9 PE
MySQL

*Normalizing/
Forwarding Agents:*
lin-hlogd
lin-ulogd
sysevt



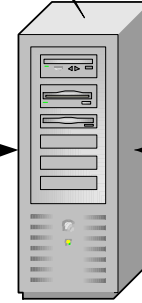
cmu5
10.54.2.6/24
Windows 2000 Server

*Normalizing/
Forwarding Agents:*
win-appd
win-hlogd
win-ulogd
win-slogd
sysevt



cmu6
10.54.2.7/24
Red Hat 9 PE

*Normalizing/
Forwarding Agents:*
netflowd
snortd
sysevt



cmu4
10.54.2.5/24
Red Hat 9 PE
MySQL

*Normalizing/
Forwarding Agents:*
sysevt

Storage Agent:
ccBay-sqlize

Storage/Forwarding Agent:
storforwd

Application Agents:
ccBay-query
ccBay-webconsole
lin-xmlevt



cmu8
10.54.2.9/24
Red Hat 9 PE

*Normalizing/
Forwarding Agents:*
lin-hlogd
lin-ulogd
sysevt

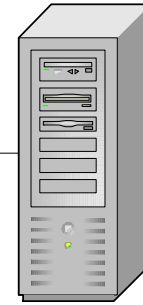


cmu7
10.54.2.8/24
Windows Server 2003 EE

*Normalizing/
Forwarding Agents:*
sysevt

Storage/Forwarding Agent:
storforwd

Application Agent:
win-xmlevt



cmu9
10.54.2.10/24
Red Hat 9 PE

*Normalizing/
Forwarding Agents:*
lin-hlogd
lin-ulogd
sysevt

Normalizing/Forwarding Agents:

sysevt: ccBay internal application events
apached: Apache Web server application events
netflowd: NetFlow flow network events
snortd: Snort intrusion detection security events
lin-hlogd: Linux host level system events
lin-ulogd: Linux user level application events

Normalizing/Forwarding Agents:

win-appd: Windows installed software application events
win-hlogd: Windows host level system events
win-ulogd: Windows user level application events
win-slogd: Windows security level system events

Storage Agent:

ccBay-sqlize: Stores events in MySQL database

Storage/Forwarding Agent:

storforwd: DB storing, archiving, tagging and forwarding

Application Agents:

ccBay-query: DB query and search CLI utility
ccBay-webconsole: DB query and search Web application
lin-xmlevt: Linux event viewer Web application
win-xmlevt: Windows event viewer Web application