Monitoring your Network with Linux
Agenda

- Why monitor the network?
- Hobbit Network Monitor
- Hobbit concepts
- Installing and configuring Hobbit
- Extending Hobbit
- Hobbit operations
Why monitor the network?

• Monitoring packages available for our systems
  – CICS, VSE, VM, Linux
  – Designed to monitor internals (tasks, jobs)
• Networks are getting more complex
• Systems are very interconnected
• We rely much more on varying types of systems
Why monitor the network?

- Many machines perform 'business critical' functions
- Network administrators need to know when these systems are down
  - Or running degraded
- Notification of administrators off shift
Hobbit Network Monitor

- Network availability monitor
- Web based display
- Uses colored icons and backgrounds
- Can perform any number of tests on any number of hosts
- Reports test results as a state
  - Up, down, on, off, red, green
- Marginal state used for impending trouble
  - yellow
Hobbit Network Monitor

• Network tests run every 5 minutes
• The web page updates are done every minute
• If a test fails, it is re-tested every minute for 30 minutes
  – Reduces the need to change the test time
Hobbit History

- Originally called 'bb-gen toolkit'
- Offered as an enhancement to Big Brother (http://bb4.com)
- Big Brother runs on various Unix systems
  - Implemented almost entirely as shell scripts
  - Easy to write and fairly universal, but not the best performance
  - Not an open source license
  - Development focused on commercial product
- bb-gen reimplemented the core of bb in C
Hobbit History

- Development of the 'free' version of bb stagnated
- Henrik Stoerner evolved bb-gen into a stand-alone package
- Hobbit 4.0 was released on Mar 31, 2005
- Very active development
  - 4.0.3 is current
Hobbit features

- Developed to monitor thousands of hosts
  - Handles big or small networks with ease
- Text file configuration
  - Web based configuration is planned
- Notification feature
  - Email (including cell phone), SMS
- Extensible through external scripts or clients
Hobbit features

- Networked applications can be monitored
  - Connections are mimicked and typical responses watched
- Common protocols are available
  - FTP, Telnet, HTTP, DNS, LDAP, SMTP, etc
  - SSL testing of any protocols
- Testing of multiple servers can be combined into a single report
Hobbit features

• “Green is good, Red is bad”
  – Simple web based front end
• Hosts can be grouped together
  – Based on logical or physical relationships
  – Groups can be in separate sections, web pages or both
• Tests for certain hosts can be on a separate page specifically suited to a NOC.
Hobbit features

- In addition to HTML...
  - PDAs can be used via WAP/WML
  - RSS Feeds can be set up
  - XML format is also available
- Integrated trend analysis via LARRD
  - Generates graphs
- Event history is available
  - Can be used for SLA reporting
- Hosts can be disabled for planned downtime
Hobbit installation

- Fairly standard Linux application install
  - RPMs available for x86 architecture
  - Source RPMs available
  - Source also available via tarball

- Available from

- If installing on x86, use the RPM

- For zSeries, install the source RPM
  - Or 'build your own'
Hobbit installation

• Prerequisites
  – A Unix-like operating system
  – Apache webserver
  – Working compiler and GNU make
  – PCRE, RRDTool, libpng and fping
    • Regular expression matching
    • Graphing
    • Fast connection test
  – For SSL support
    • Open SSL
  – For LDAP support
    • Open LDAP
Hobbit installation

• Create a 'hobbit' user
• Use RPM or configure/make to build
• During the configuration, a number of questions are asked
  – The defaults are sensible
  – Only had to answer the location of fping and IP address prompts
• Use make to build the package
• As root 'make install'
Apache configuration

- An Apache configuration file is included with Hobbit
  - ~/server/etc/hobbit-apache.conf
- Copy to /etc/apache2/sysconfig.d
- Edit /etc/sysconfig/apache2
  - Put the local hostname in APACHE_SERVERNAME
  - The path to the configuration file in APACHE_CONF_INCLUDE_FILES

APACHE_CONF_INCLUDE_FILES=/etc/apache2/sysconfig.d/hobbit-apache.conf
Apache configuration

- Start Apache
  - /etc/rc.d/apache2 start
- Test access to webserver
- Set up Apache to start at boot
  - chkconfig apache2 on
  - YaST
- Use htpasswd to create users for access secured
  Hobbit administration functions
Hobbit startup

- Sign on as 'hobbit' user
- Use the command
  - ./server/hobbit.sh start
- The response should be 'Hobbit started'
- A number of process will be running
  - An explanation of what they do is in the documentation
- After a few minutes use your web browser to navigate to your Hobbit server
  - http://192.168.201.12/hobbit/
Hobbit web page
Hobbit web page

- Provides the status of the Hobbit server
- Clicking on an icon provides more information
- Including trending graphs
Hobbit web page

Wed Apr 20 14:23:01 2005

bbgen version 4.0 with hobbitdb

<table>
<thead>
<tr>
<th>Statistic</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>5</td>
</tr>
<tr>
<td>Status messages</td>
<td>42</td>
</tr>
<tr>
<td>Purple messages</td>
<td>0</td>
</tr>
<tr>
<td>Pages</td>
<td>3</td>
</tr>
</tbody>
</table>

**TIME SPENT**

- Event                      | Starttime | Duration |
- Startup                    | 11:40:24  | 0:00:20  |
- Load links done            | 11:40:24  | 0:00:20  |
- Load bbgen done            | 11:40:24  | 0:00:20  |
- 4K removal done            | 11:40:24  | 0:00:20  |
- Load START done            | 11:40:24  | 0:00:20  |
- Color calculation done     | 11:40:24  | 0:00:20  |
- BB pagegen start           | 11:40:24  | 0:00:20  |
- BB pagegen done            | 11:40:24  | 0:00:20  |
- BB2 generation done        | 11:40:24  | 0:00:20  |
- BBIR generation done       | 11:40:24  | 0:00:20  |
- Summary Transmission done  | 11:40:24  | 0:00:20  |
- Run completed              | 11:40:24  | 0:00:20  |

**TIME TOTAL**

- 0:00:20

Status unchanged in 3 days, 15 hours, 4 minutes
Status message received from 192.168.201.12

hobbit bbgen Runtime Last 48 Hours

Run Time:
- 0.4 (cur)
- 0.6 (max)
- 0.3 (min)
- 0.4 (avg)

Updated: 20-Apr-2005 14:23:14
Configuring Hobbit

- Configuration involves editing text files
  - Web based configuration is planned
- Primarily ~/server/etc/bb-hosts
- Changes automatically take affect during the next test cycle
Hobbit configuration file

```
group Hobbit Servers
192.168.201.12   hobbit       # BBDISPLAY BBPAGER BBNET bbd http://hobbit/
group Linux for zSeries
192.168.201.8    conn2       # ftp dialup
192.168.201.9    db2b        # ftp NK:ftp
group VM/VSE systems
192.168.201.1    vm1         # ftp NK:conn,procs
192.168.201.2    vse1        # dialup
```
Hobbit configuration file

**group Hobbit Servers**
192.168.201.12   hobbit      # BBDISPLAY BBPAGER BBNET bbd http://hobbit/

**group Linux for zSeries**
192.168.201.8    conn2       # ftp dialup
192.168.201.9    db2b        # ftp NK:ftp

**group VM/VSE systems**
192.168.201.1    vm1         # ftp NK:conn,procs
192.168.201.2    vse1        # dialup
Hobbit configuration file

```
group Hobbit Servers
192.168.201.12   hobbit      # BBDISPLAY BBPAGER BBNET bbd http://hobbit/
group Linux for zSeries
192.168.201.8    conn2       # ftp dialup
192.168.201.9    db2b        # ftp NK:ftp
group VM/VSE systems
192.168.201.1    vm1         # ftp NK:conn,procs
192.168.201.2    vse1        # dialup
```

Host name of a monitored host
depends on fully qualified or not
Hobbit configuration file

Directives used for Big Brother compatibility
Hobbit configuration file

Identifies this system as the hobbit server
Hobbit configuration file

- **group Hobbit Servers**
  - 192.168.201.12 hobbit
  - 192.168.201.8 conn2
  - 192.168.201.9 db2b

- **group Linux for zSeries**
  - 192.168.201.1 vm1
  - 192.168.201.2 vse1

- **group VM/VSE systems**
  - 192.168.201.1 vm1

- **Monitor Hobbit's own web site**
  - [http://hobbit/](http://hobbit/)
Monitor ftp on conn2, db2b and vm1
Hobbit configuration file

group Hobbit Servers
192.168.201.12 hobbit          # BBDISPLAY BBPAGER BBNET bbd http://hobbit/
group Linux for zSeries
192.168.201.8 conn2            # ftp dialup
192.168.201.9 db2b             # ftp NK:ftp
group VM/VSE systems
192.168.201.1 vm1             # ftp NK:conn,procs
192.168.201.2 vse1            # dialup

Treat conn2 and vse1 as dialup links
If they are unreachable, no notifications
Hobbit configuration file

Special directive for the NK View page
Hobbit configuration file

Group the following hosts
'Page' will create a separate web page
Host or service failure

- Detected by Hobbit during its network test cycle
- Turns the icon and web page background red
- Shows 'red' in the web page title bar
- Notifies appropriate administrator via email or page
### Hobbit Servers

<table>
<thead>
<tr>
<th>Server</th>
<th>hbd</th>
<th>bbgen</th>
<th>hbtest</th>
<th>conn</th>
<th>hobbitd</th>
<th>http</th>
<th>info</th>
<th>trends</th>
</tr>
</thead>
<tbody>
<tr>
<td>hobbit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Linux for zSeries

<table>
<thead>
<tr>
<th>Server</th>
<th>conn</th>
<th>ftp</th>
<th>info</th>
<th>trends</th>
</tr>
</thead>
<tbody>
<tr>
<td>conn2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db2b</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### VM/VSE systems

<table>
<thead>
<tr>
<th>System</th>
<th>conn</th>
<th>cpu</th>
<th>ftp</th>
<th>getvis</th>
<th>info</th>
<th>paging</th>
<th>pg_util</th>
<th>procs</th>
<th>sp_util</th>
<th>trends</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vse1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vse2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Other views of the network

• Three different views
  – Main View
  – All non-green view
    • All systems that are currently not green
    • Shows last 6 hours or last 25 state transitions
  – NK view
    • Systems currently not green identified by NK tag
All Monitored Systems OK

5 events received in the past 75 minutes

Fri Apr 22 16:37:12 2005 db2b ftp
Fri Apr 22 15:41:57 2005 db2b ftp
Fri Apr 22 15:36:54 2005 db2b ftp
Fri Apr 22 15:21:46 2005 db2b ftp
Fri Apr 22 15:21:46 2005 db2b conn

No events acknowledged in the last 240 minutes
Current Critical Systems

ftp    info    trends

db2b  🅿️  🟢  🟢

Hobbit Monitor 4.0
Host or service return

- When a host or service becomes available
- Icons and page background turn green
- An optional notification can be sent out
- Non-green page shows the transition
Extending Hobbit

- Hobbit provides a lot of information by itself
- Designed to retain compatibility with Big Brother
- Big Brother has a large number of 'add-on' packages and clients for other operating systems
Extending Hobbit

• Big Brother extensions are available at http://www.deadcat.net

• Community contributions to extend/improve monitoring

• A large number of categories of packages
  – Backup, Clusters, Databases, LDAP, Windows, performance, processes, SNMP, disk, email, files, memory, RAID, power, security, routers, logging, NFS, skins
Extending Hobbit

• The majority of these should be compatible with Hobbit

• Clients for other operating systems
  – OS/400
  – OS/390 z/OS
  – Netware
  – Alpha OpenVMS
  – z/VM
Extending Hobbit

• z/VM client
  – Runs in a virtual machine
  – Written in REXX
  – Reports CPU Utilization, Paging, Page and Spool Utilization and running virtual machines
Extending Hobbit

• z/OS client
  – Runs as a started task
  – Written in REXX and assembler
  – Reports CPU Utilization, Spooling, Paging, running processes, disk volume utilization, storage
Extending Hobbit

- Hobbit provides a well defined interface for reporting status messages
  - The same interface Big Brother used
  - Status can be reported
    - Locally (on the Hobbit server) via a command
    - Via a socket connection over port 1984

- Open a socket to the Hobbit server

- Send a status message:

  status vml.cpu green 30 Mar 2005 08:20:06   CPU Utilization  25%
  z/VM Version 4, Release 4.0, service level 0402 (32-bit)
  AVGPROC-025%  01
28 Apr 2005 15:27:23 CPU Utilization 31%

z/VM Version 4 Release 4.0, service level 0402 (32-bit)
AVGPROC=031% 01

Status unchanged in 28 days, 5 hours, 47 minutes
Status message received from 192.168.201.1

hobbit graph l.a
When clients don't respond

- Hobbit expects clients to communicate at regular intervals
- Most default to the standard Hobbit interval of 5 minutes
- If a status report is not received after 30 minutes, Hobbit turns the client tests purple
- If properly configured a notification will be sent out
- Green is restored when the client is restarted
Hobbit operations

- Starting and stopping
- Outage notification
- Alert Acknowledgment
- Enable/Disable
- Reporting
Starting and stopping Hobbit

- The traditional Linux start/stop process can be used
- Script is not provided, easy to create
- Copy existing script (like cron) to hobbit
- Will appear in output of `chkconfig --list` so that startup can be turned on or off
Starting and stopping Hobbit

#!/bin/sh
### BEGIN INIT INFO
# Provides:    hobbit
# Required-Start: network
# Required-Stop: network
# Default-Start: 3 5
# Default-Stop: 3
# Description: Start the hobbit network monitor
### END INIT INFO

case "$1" in
  start)
    echo "Starting Hobbit"
    su - hobbit -c "cd /home/hobbit/server; ./hobbit.sh start"
    ;;
  stop)
    echo "Stopping Hobbit"
    su - hobbit -c "cd /home/hobbit/server; ./hobbit.sh stop"
    ;;
  restart)
    $0 stop
    $0 start
    rc_status
    ;;
  *)
    echo "Usage: $0 {start|stop|restart}"
    exit 1
    ;;
esac
Outage Notification

- A page or email is sent out when a non-green condition occurs
- Most cell phones are email capable
- Very configurable and flexible
- Very good information in the docs
- Configuration data in
  ~/server/etc/hobbit-alerts.cfg
- File contains rules about the host and service and who is notified
Outage Notification

• Simple example

    HOST=vse2
    MAIL rsmrcina@vmassist.com

• Sends an email to rsmrcina@vmassist.com if any test related to vse2 fails
Outage Notification

Subject: Hobbit [317353] vse2:procs CRITICAL (RED)
From: Hobbit <hobbit@wi.rr.com>
Date: 08:39 AM
To: rsmrcina@vmassist.com

red 28 Apr 2005 08:34:34 There are 5 jobs running.
CICSICCF Running
BSTTITAM Running
CICS1 Not running

See http://hobbit/hobbit-cgi/bb-hostsvc.sh?HOSTSVC=vse2.procs
Outage Notification

- SERVICE – notify for one or more services
  - SERVICE=conn,http,ftp

- REPEAT – repeat notification, default 30m
  - REPEAT=1h

- TIME – time range for notification
  - TIME=*:0730:2100

- COLOR – only notify for certain color
  - COLOR=red
Outage Notification

- **DURATION** – Only alert if outage is longer than time indicated
  - DURATION>10m
  - DURATION<2h

- **RECOVERED** – Sends alert when host/service returns

- **SCRIPT** – Used to code alternative alert mechanism, eg. SMS page
Outage Notification

• Wildcards can be used in the hostname and service name
  - HOST=%(www|intranet|support|mail).foo.com

• To save typing, macros are supported
  - $ZLINUX=%(conn2|db2b) $VSE=%(vse1|vse2)
  - Anywhere a macro is used, it is replaced
  - Works with recipients also
  - $ZSUPPORT=%(rsmrcinaljdoe|helpdesk)@vmassist.com
Outage Notification

HOST=conn2,db2b

MAIL rsmrcina@vmassist.com
MAIL jdoe@vmassist.com
MAIL helpdesk@vmassist.com

$ZLINUX=%(conn|db2b)

$ZSUPPORT=%(rsmrcina|jdoe|helpdesk)@vmassist.com

HOST=$ZLINUX
MAIL $ZSUPPORT
Alert Acknowledgment

• An administrator can acknowledge an alert
  – Stops notification
  – Changes web page
  – Let's users know that a resolution is near

• Each alert includes an acknowledgment code
Alert Acknowledgment

- On the Hobbit 'Administration Menu' click Acknowledge Alert
Alert Acknowledgment

- Enter
  - Duration of outage
  - Explanation
  - Acknowledgment code
- Hit Send
- Red icon turns to a check mark to indicate acknowledgment
Thu Apr 28 13:29:39 2005 conn NOT ok

Service conn on vse2 is not OK: Host does not respond to ping

System unreachable for 3 poll periods (428 seconds)

192.168.201.3 is unreachable

Status unchanged in 0 hours, 7 minutes
Status message received from 192.168.201.12
Current acknowledgment: System abend
Acked by: rts0 (192.168.1.101)
Next update at: 14:25 2005-04-28
Enable/Disable

- Stop or start the test for a service
- Use for planned outages
Enable/Disable

- Select the host and test to disable
- Enter a reason and timeframe
- Indicate whether to disable now or schedule for another time
- Press disable button
Big Brother Disabling and Enabling

Status

Processing...

Disabled [conn2.conn] on [192.168.201.12]
Disabled [conn2.hp] on [192.168.201.12]

Currently Disabled Tests

<table>
<thead>
<tr>
<th>Enable?</th>
<th>Host</th>
<th>Test</th>
<th>Offline Until</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>conn2</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Check All

All tests for each selected host will be re-enabled

Re-enable

Scheduled Disabled Tests ("at" queue on hobbit)

None

Hosts

<table>
<thead>
<tr>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
</tr>
<tr>
<td>conn2</td>
</tr>
<tr>
<td>db2b</td>
</tr>
<tr>
<td>hobbit</td>
</tr>
<tr>
<td>vm1</td>
</tr>
<tr>
<td>vse1</td>
</tr>
<tr>
<td>vse2</td>
</tr>
</tbody>
</table>

Tests

Pick a host...

Reason: 

Username: rks0 at 192.168.200.253

Duration: 4 hours

Disable Now

Schedule for Disable

Year: 2005
Month: 05
Day: 19
Hour: 20
Min: 57

Disable
Reset
Hobbit reports

- Event Log report is similar to the non-green view
  - You can control how far back to go
  - You can control how many events to show
How long to go back in time: 6000 minutes
Max. number of events: 100

View log
Hobbit reports

• Availability report will show the percentage of time that each host and service is available

• Enter a date range and one of three options
  – Critical events (red)
  – Non-green events
  – All events
<table>
<thead>
<tr>
<th>Hobbit Servers</th>
<th>bbd</th>
<th>bbgen</th>
<th>bbtest</th>
<th>conn</th>
<th>hobbitd</th>
<th>http</th>
</tr>
</thead>
<tbody>
<tr>
<td>hobbit</td>
<td>⬆️</td>
<td>⬆️</td>
<td>⬆️</td>
<td>⬆️</td>
<td>⬆️</td>
<td>99.98</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Linux for zSeries</th>
<th>conn</th>
<th>ftp</th>
</tr>
</thead>
<tbody>
<tr>
<td>conn2</td>
<td>⬆️</td>
<td>⬆️</td>
</tr>
<tr>
<td>db2b</td>
<td>⬆️</td>
<td>90.82 99.45</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VM/VSE systems</th>
<th>conn</th>
<th>cpu</th>
<th>ftp</th>
<th>getvis</th>
<th>paging</th>
<th>pg_util</th>
<th>procs</th>
<th>sp_util</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm1</td>
<td>⬆️</td>
<td>⬆️</td>
<td>⬆️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>vse1</td>
<td>⬆️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>vse2</td>
<td>⬆️</td>
<td>-</td>
<td>-</td>
<td>⬆️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>99.77</td>
</tr>
</tbody>
</table>
Hobbit reports

- Snapshot report
  - A point in time image of how the Hobbit web page looked at a point in the past
  - Enter a date and time
Hobbit Snapshot Report

Generate Report

Hobbit Monitor 4.0
### Hobbit Servers

<table>
<thead>
<tr>
<th>Hobbit Servers</th>
<th>bbd</th>
<th>bbgen</th>
<th>bbtest</th>
<th>conn</th>
<th>hobbild</th>
<th>http</th>
</tr>
</thead>
<tbody>
<tr>
<td>hobbit</td>
<td>'+'</td>
<td>'+'</td>
<td>'+'</td>
<td>'+'</td>
<td>'+'</td>
<td>'+'</td>
</tr>
</tbody>
</table>

### Linux for zSeries

<table>
<thead>
<tr>
<th>Linux for zSeries</th>
<th>conn</th>
<th>ftp</th>
</tr>
</thead>
<tbody>
<tr>
<td>conn2</td>
<td>'+'</td>
<td>'+'</td>
</tr>
<tr>
<td>db2b</td>
<td>'+'</td>
<td>'+'</td>
</tr>
</tbody>
</table>

*conn:red:* 10.10 minutes

### VM/VSE systems

<table>
<thead>
<tr>
<th>VM/VSE systems</th>
<th>conn</th>
<th>cpu</th>
<th>ftp</th>
<th>getvis</th>
<th>pacing</th>
<th>pg_util</th>
<th>proc</th>
<th>sp_util</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm1</td>
<td>'+'</td>
<td>'+'</td>
<td>'+'</td>
<td>'-'</td>
<td>'-'</td>
<td>'+'</td>
<td>'+'</td>
<td>'+'</td>
</tr>
<tr>
<td>vse1</td>
<td>'+'</td>
<td>'-'</td>
<td>'-'</td>
<td>'-'</td>
<td>'-'</td>
<td>'-'</td>
<td>'+'</td>
<td>'+'</td>
</tr>
<tr>
<td>vse2</td>
<td>'-'</td>
<td>'-'</td>
<td>'-'</td>
<td>'+'</td>
<td>'+'</td>
<td>'-'</td>
<td>'-'</td>
<td>'+'</td>
</tr>
</tbody>
</table>

*conn:red:* 10.10 minutes

---

http://192.168.201.12/hobbit-cgi/bb-histlog.sh?HOST=db2b&SERVICE=conn&TIMEBUF=Sat_Apr_23_08:34:54_2005
Wrapping up...

- Enterprise class monitoring solution
- Open Source
- Under heavy development, but feature rich
- Runs on Linux (including zSeries!)
- Can be well integrated into the zSeries environment
- Easy to install and configure
- Expandable, very useful and performs well
Questions...

Rich Smrcina
rsmrcina@vmassist.com