

Centralised patch management

J. Barhorst & M. Pels
July 5, 2005

What did we do?

Contents

- Activities
- Comparison
- Requirements
- Proof of Concept
- Conclusion

- Look at client update tools
- Create list of research topics
- Investigate three existing patch management systems
- Compose list of functional requirements for ideal patch management
- Build Proof of Concept

Existing systems

Contents

- Activities
- ➔ Comparison
- Requirements
- Proof of Concept
- Conclusion

Area	WSUS	Radia	LANDesk
Patches	+	+	+
End users	+	++	++
Distribution	0	+	+
Administration	+	+	+
User interface/Framework	++	0	+
Infrastructure	0	++	+
Reporting	0	+	0

Contents

- Activities
- Comparison
- ➔ Requirements
- Proof of Concept
- Conclusion

Ideal requirements (1/5)

Patches:

- Acquire via existing mechanisms or a third party
- Rollback capability
- Verification (digital signature, checksum)
- Multi-platform
 - ➔ Impossible to support everything
 - ➔ Multiple PMS's is not a bad thing

Contents

- › Activities
- › Comparison
- Requirements
- › Proof of Concept
- › Conclusion

Ideal requirements (2/5)

End users:

- Should not be able to reject or rollback patches
- Reboot options should be versatile:
 - Warning
 - Postpone
 - Deadline
 - After office hours

Ideal requirements (3/5)

Contents

- › Activities
- › Comparison
- Requirements
- › Proof of Concept
- › Conclusion

Distribution:

- Agent & existing mechanisms
- Prioritization (based on risk / severity)
- Grouping of hosts (servers / workstations)
- “One, some, many”

Administration:

- Approve / reject patches
- Custom patches / scripts

Ideal requirements (4/5)

Contents

- Activities
- Comparison
- Requirements
- Proof of Concept
- Conclusion

User interface / Framework:

- User-friendliness
- Access control
- Backups / restore
- More information about patches (CVE)

Infrastructure:

- Multicast / peer-to-peer / multiple servers
- Low / expensive bandwidth users
- Inventory building

Contents

- Activities
- Comparison
- ➔ Requirements
- Proof of Concept
- Conclusion

Ideal requirements (5/5)

Reporting:

- Alerting (SMS, e-mail, etc)
- Reports
 - ➔ Patches (succes, failure, new, rejected, etc)
 - ➔ Hosts (completely patched, missing patches)
 - ➔ Groups (hosts, approved patches)
 - ➔

Proof of Concept

Contents

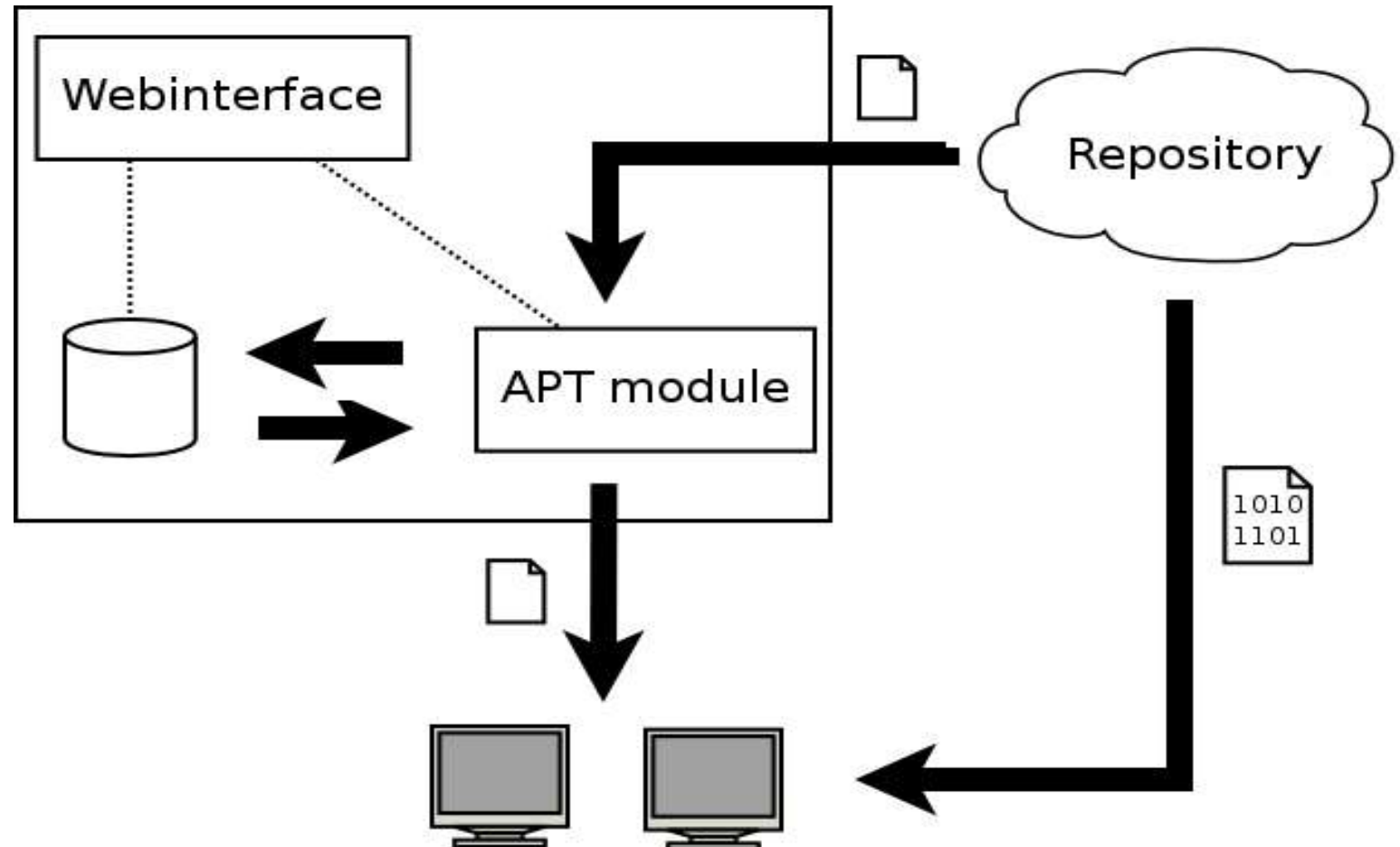
- › Activities
- › Comparison
- › Requirements
- Proof of Concept
- › Conclusion

- Why a Proof of Concept?
- Why APT?
- Why Ubuntu?

Components

Contents

- Activities
- Comparison
- Requirements
- ➔ Proof of Concept
- Conclusion



APT module

Contents

- › Activities
- › Comparison
- › Requirements
- Proof of Concept
- › Conclusion

- Synchronize
 - Download Package & Release file
 - Verify signature & checksums
 - Store package info in database
- Build
 - Retrieve package info from database
 - Make new Package & Release file
 - Create digital checksums & signature

Conclusion

Contents

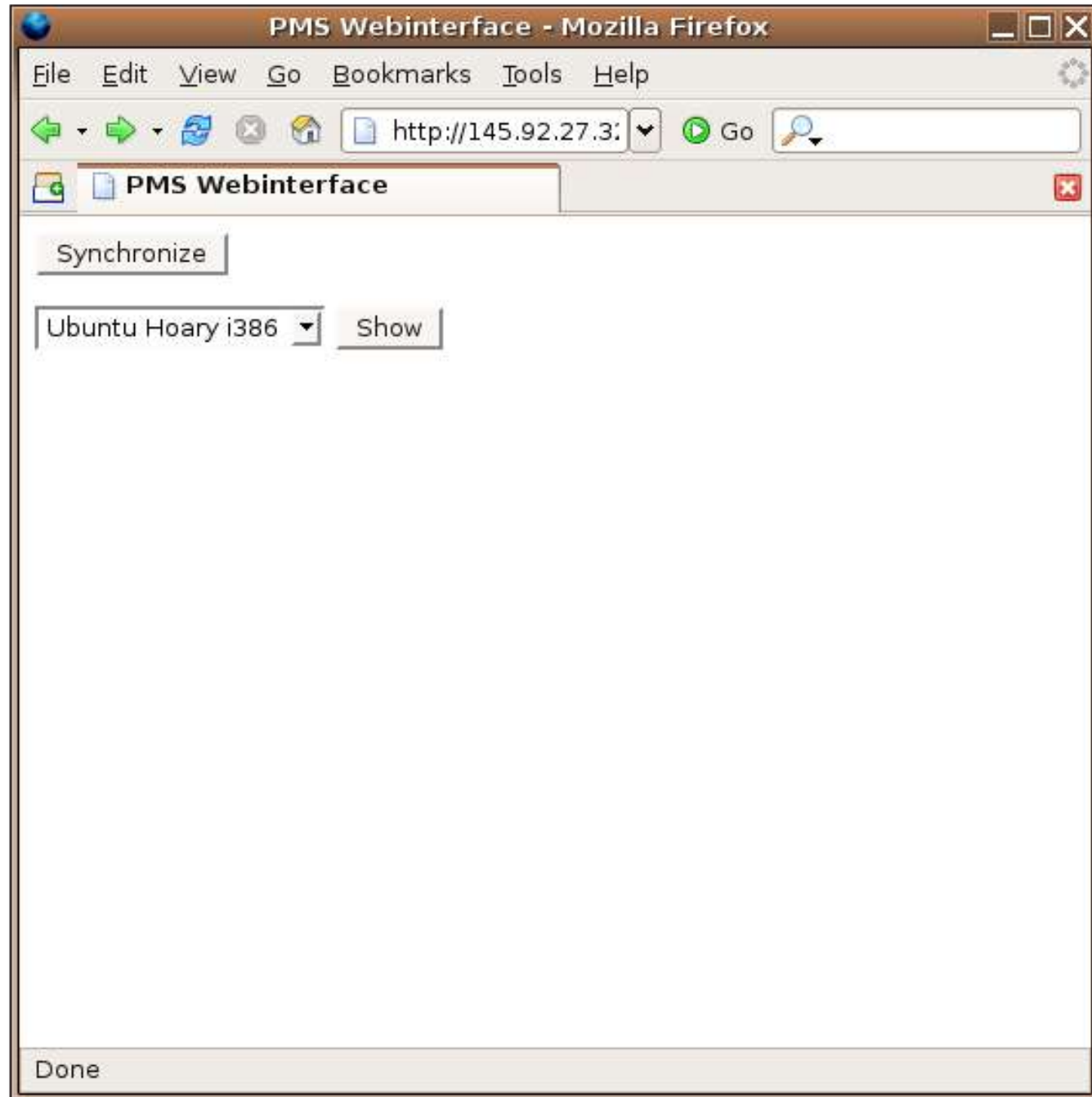
- › Activities
- › Comparison
- › Requirements
- › Proof of Concept
- Conclusion

- Product investigation
- Ideal requirements
- Proof of Concept

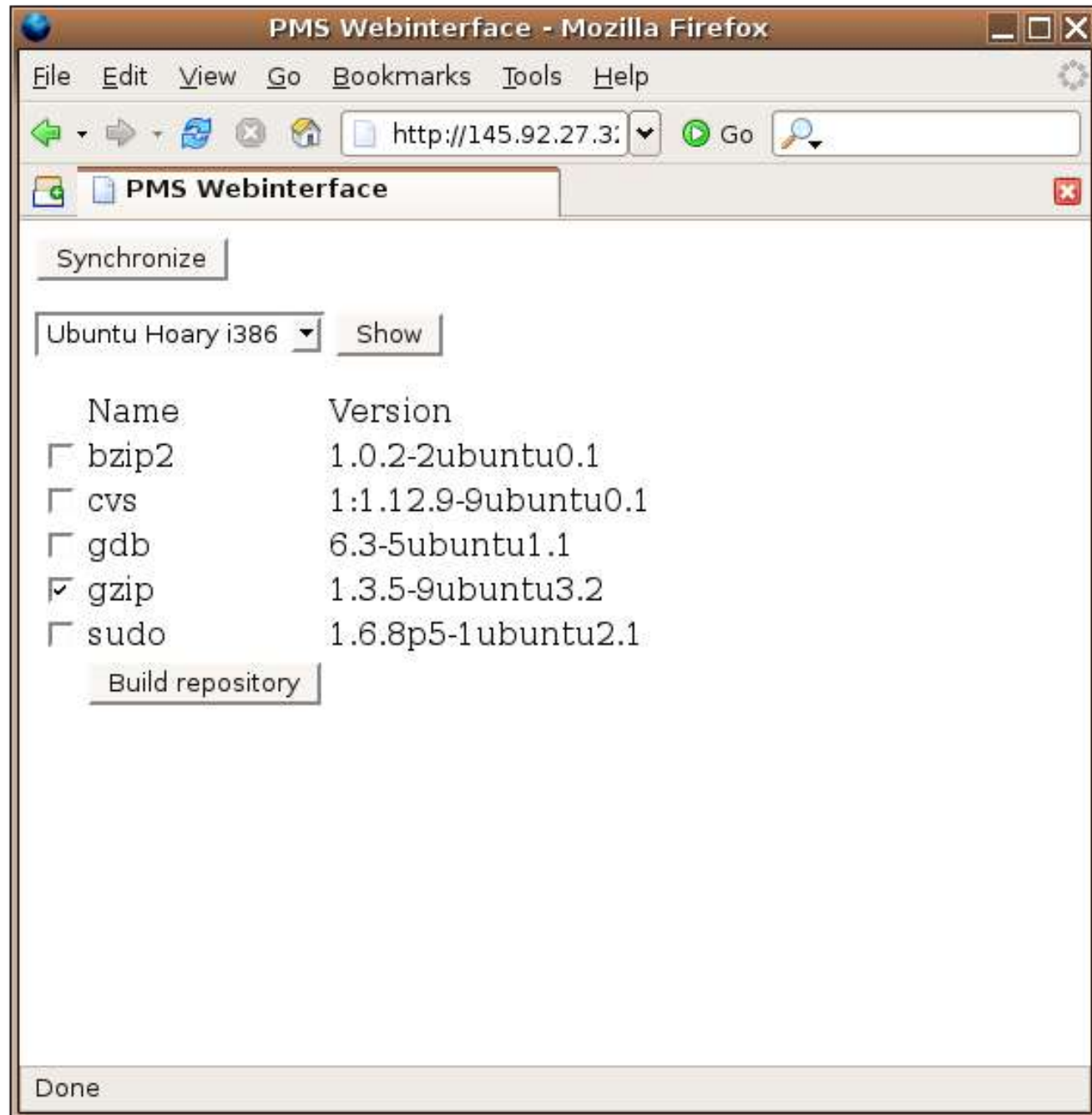
- Future work

Questions?

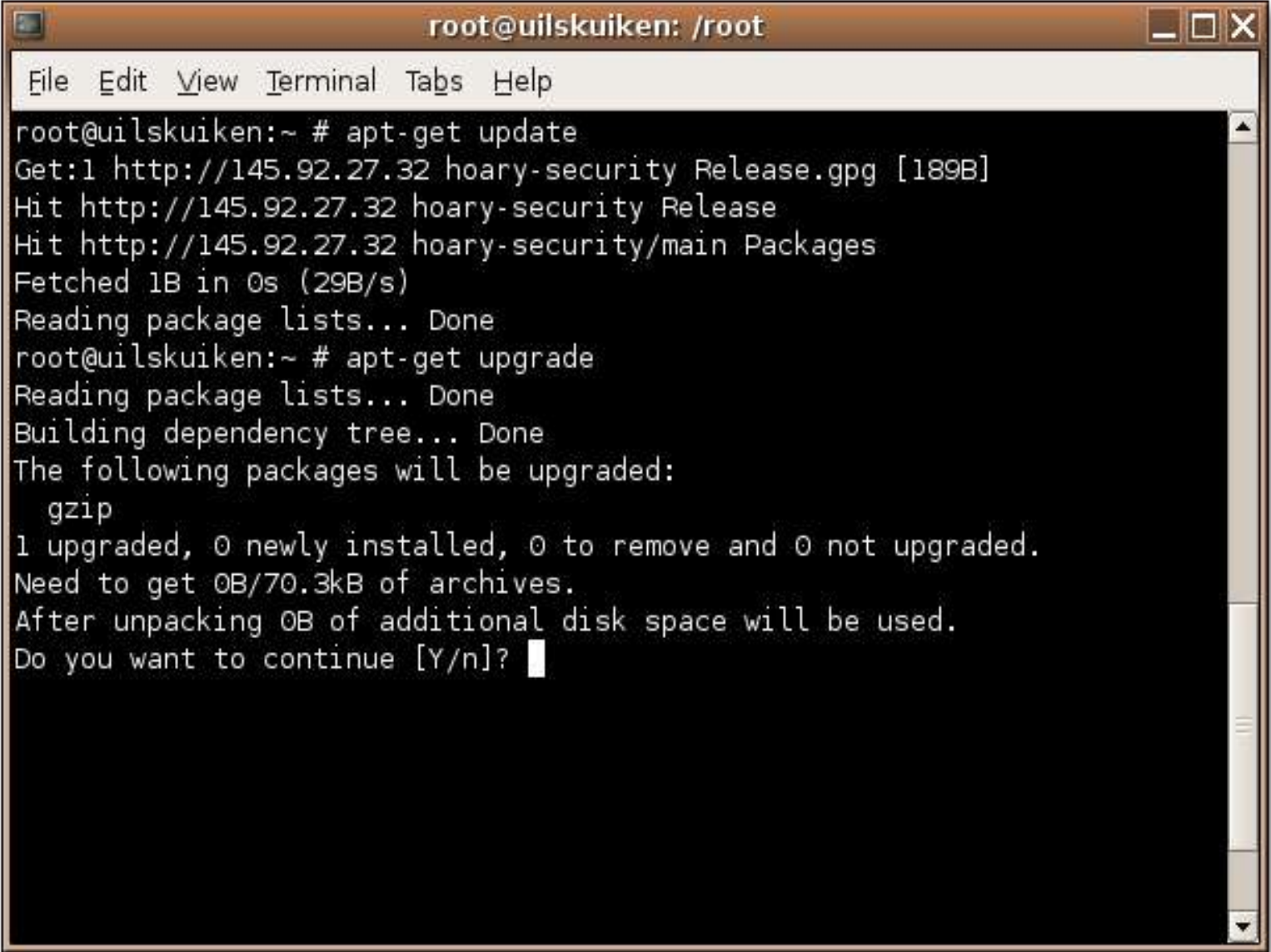
Screenshots (1/3)



Screenshots (2/3)



Screenshots (3/3)



```
root@uilskuiken: /root
File Edit View Terminal Tabs Help
root@uilskuiken:~ # apt-get update
Get:1 http://145.92.27.32 hoary-security Release.gpg [189B]
Hit http://145.92.27.32 hoary-security Release
Hit http://145.92.27.32 hoary-security/main Packages
Fetched 1B in 0s (29B/s)
Reading package lists... Done
root@uilskuiken:~ # apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
The following packages will be upgraded:
  gzip
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 0B/70.3kB of archives.
After unpacking 0B of additional disk space will be used.
Do you want to continue [Y/n]? █
```