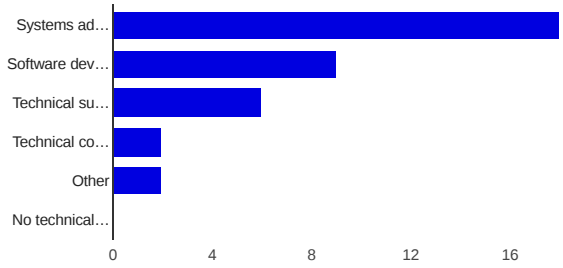
[redacted] Edit this form

20 responses

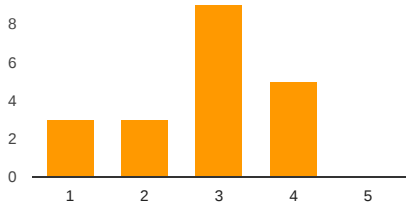
Summary

Please indicate your technical background



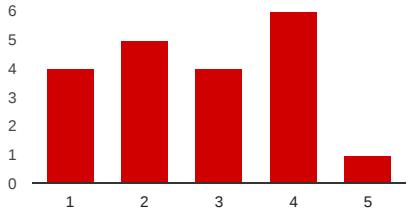
Systems administrator	**18**	90%
Software developer	**9**	45%
Technical support	**6**	30%
Technical communications / documentation	**2**	10%
Other	**2**	10%
No technical background	**0**	0%

****Prior to the workshop** what was your level of familiarity with identity management technologies (LDAP, Kerberos, PKI, etc)?**



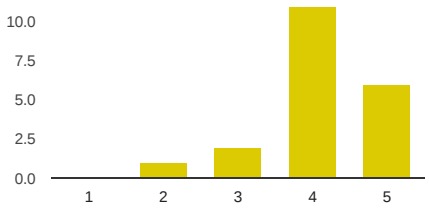
Not at all familiar: 1	**3**	15%
2	**3**	15%
3	**9**	45%
4	**5**	25%
Guru: 5	**0**	0%

****Prior to the workshop** how likely would you have been to deploy or recommend FreeIPA for your organisation / project?**



Would never recommend: 1	**4**	20%
2	**5**	25%
3	**4**	20%
4	**6**	30%
Highly likely to recommend: 5	**1**	5%

****After the workshop** how likely are you to deploy or recommend FreeIPA for an organisation / project?**

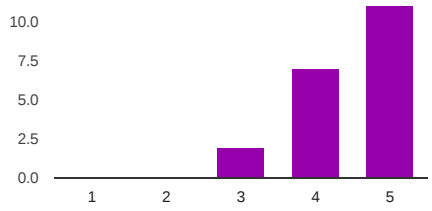


Would never recommend: 1	**0**	0%
2	**1**	5%
3	**2**	10%
4	**11**	55%
Highly likely to recommend: 5	**6**	30%

Please rate the quality of the workshop orientation presentation

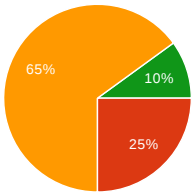
Very poor: 1	**0**	0%
2	**0**	0%
3	**2**	10%
4	**9**	45%
Very good: 5	**9**	45%

Please rate the usefulness of the workshop preparation instructions and resources



Useless: 1	**0**	0%
2	**0**	0%
3	**2**	10%
4	**7**	35%
Prepared me perfectly for the workshop: 5	**11**	55%

Please indicate how difficult you found the workshop curriculum



Too easy	**0**	0%
Easy	**5**	25%
Neither easy nor difficult	**13**	65%
Challenging	**2**	10%
Too difficult	**0**	0%

Were there any aspects of the workshop you felt worked quite well or were particularly useful to you?

I liked the method of having mostly directed instruction, but there was a mix. Having single sentence that a user must achieve using their own initiative is a great learning technique.

Particularly useful: certificates

Instructions were a nice mix of copy/paste and work it out yoruself.

documentation on the steps was top notch!!!!!!

Generally speaking the instructions and pre-prepared vagrant box were great and easy to follow. This is backed up by the ipa wizard commands.

Pre-built VMs are good, but I think it would be better to simply supply the actual packer templates used to create the pre-built VMs rather than referring to modifying the default packer templates.As it stands, it looks a little hacky, when it wouldn't be hard to supply the packer template JSON straight in the repo. (Maybe I'm biased since I hack on packer itself :))

Single Sign On

It would be good to specify the link to the pre-work near the top, rather than at the bottom, of the workshop's description. I should have read the workshop's description fully, but I skimmed it and missed the request for participants to complete the pre-work.

Hesitated previously to dive into FreeIPA (and vagrant for that matter) thinking it would be an evenings work and somehow managed to blast through the tutorial getting half way through module 5 having never setup FreeIPA (or worked with vagrant) previously.

Were there any aspects of the workshop you felt were executed poorly or not useful to you?

I think enrollment by manual instead of pre-create/OTP is somewhat a bad practice to show. I know it's just a workshop to start with, but I think it's also useful to demo some best practice as well.

nope

need to fix version in download instructions. Need to add info about sudo sss_cache -E

The replica activity only covered setting up a replica server and didn't explain the other half: how to set up clients to use (or fall back to) a replica

dbus-send command seems broken? also Vagrant networking was misbehaving on my env, so that lead to weird and wonderful hacking.

No

Were there topics **not covered during the workshop, which you would like to have been covered?**

As an advanced topic the setup of sudo would be great. Given that most people will who will deploy and use IPA will be sys admins then instruction on sudo, and the sane restriction of it is important.

Sudo management from FreeIPA

It would have been good to give an introduction to Kerberos in general, and maybe outline a case study of how enterprises are using

it.

Single Sign On to laptop or desktop computer, iLO, web-based products such as Jira, Confluence, Observium, etc.

sudo configuration. more explanation of the architecture in a practical sense (eg, certmonger issues certificates, like a CA, that you can use for TLS on your webserver, mail etc)

Cross-realm trust, even as a light demo to show. FreeIPA doesn't exist in a vacuum and I think this is a useful piece of linkage.

I think as an introduction workshop this was a good start, as a next step I would love a bit more of a deep dive including gotchas or scenarios for common production deployments. As 2FA has become very relevant and much more popular in the past 1-2 years, I feel that an extra step to setup OTP with Google Authenticator and enable that for SSH would be a fantastic addition that is practical and useful but probably not too complex to add to an otherwise fairly straight forward tutorial.

2FA - yubi neo-n in my case

Integrating IPA users with email mailboxes

Do you have any other feedback for the presenter about any aspect of the workshop?

THANK YOU!

Unfortunately I had to watch someone else because there was not a box image for my 32-bit system (although Fraser tried very hard to get me one but hardware problems defeated him).

Prep being done is always good, but it's handy to have an easy way to dump the images out to a lot of people if required. Unsure of the best way to do this, a couple of USB sticks is okay but not that quick!

I came into the tutorial without knowing much about the discussed technologies. Perhaps a more in-depth walk through would have helped.

The workshop was very well prepared and easy to follow. The only glitch was client not able to sync time with the server. I thought I would have to fix it before I could continue. Then, I made a typo in the "app" config of the pam module and couldn't figure out what was wrong. There was no error message in any log or any other indication of what was wrong. I had to re-do the module twice before I found the typo. If this happened to me in a production environment, it could take me hours to find and fix the problem, leaving hundreds of people unable to log in to systems. I find HBAC Services and HBAC Service Groups redundant and confusing. There should be only Services and Service Groups the same way there are only Hosts and Host Groups and only HBAC Rules to link them together. After the workshop, I feel confident to use FreeIPA in a small environment, e.g. a single office, and for a small number of non-business critical applications. I don't feel confident in deploying it across a large scale environment of several remote offices and several data centres where robustness and reliability is crucial. FreeIPA is quite complex and fragile. It still requires very deep understanding of each component (LDAP, Kerberos, SELinux, PAM modules, etc.) to keep it running. It should be simplified in the first place and then configuration made more automated and error prone to improve usability, increase the robustness and reduce the deployment time. Better diagnostics should be put in place to be able to identify and fix any problem immediately (e. g. a clear message in a central error log file briefly explaining what's wrong and how to fix it).

pls install the vims and the bash-completions to the base image :D

next time could lib-virt be used on both Ubuntu and Fedora please? Life is better without virtualbox :)

N/A

Great work !

Number of daily responses