OpenLDAP: DICE client configuration

This is the final report for Project 267 - OpenLDAP: DICE client configuration.

Contents

1. Introduction

The aim of this long-running project has been to review the existing configuration of OpenLDAP on the DICE system, and consider whether it could and should be changed.

See the project's homepage for resulting discussion papers etc.

2. Outcome of the project

The project has concluded that:

1. We will move to a conventional distributed LDAP configuration for all DICE clients (†), and will only revert from this decision if some major technical obstacle or blocking issue comes to light.
2. We will allow special-casing of certain clients: DICE machines will be allowed to run their own LDAP servers (replicating from the master via `syncrepl`) where this is judged to be either necessary or prudent. We expect the number of such cases to be small.
3. The move to the new configuration will be arranged at the time of the next DICE OS upgrade (i.e. the expected upgrade to SL7).
4. Client-side LDAP caching will be implemented, with the clear expectation that this will be managed using `sssd`.

(† A 'DICE client' is any machine other than a designated LDAP server.)

3. Future work

Testing of the above arrangements has been going on in 'live' form on CO desktop machines for over a year, and we are confident that the above decisions are sound. However, in order to finally effect the above changes, there remains significant operational work, development work, and testing to be done. The work of this project has been to consider the issues, and to prototype and test the suggested configuration; we expect all future work to be done

either operationally, or as part of the overall SL7 upgrade project.

The minutes of the meeting at which the decision to move to a new LDAP configuration was taken summarize some of the work remaining, but it is worth emphasising a few points here:

1. We need to get LDAP caching via `sssd` fully working on DICE. (This is being addressed as part of the Infrastructure Unit's SL7 upgrade project.)
2. We need to consider both load-testing and load-balancing and as we finally roll out the new LDAP configuration to all clients. We have no way of yet knowing how many LDAP servers we will need for satisfactory performance, or indeed on what platforms (actual hardware, or VMs) such servers will run.
3. In order to avoid nasty surprises and to allow us to spot problems caused by actual load, it might be wise for use to stage the changeover to the new configuration if we can. For example, we might consider converting one computing lab at a time, and monitoring the load at each stage.
4. Each of our servers/services needs to be qualified/tested by their managers for their behaviour in the temporary absence of an LDAP service.
5. The effects of the new LDAP configuration on machines used for on-line exams need to be carefully considered by the COs responsible for those machines.
6. We need to be sure that we handle all future DICE CA root certificate upgrades seamlessly, with no detrimental effect on LDAP clients. (Updating the root certificate in this way was successfully tested in late 2013.)
7. We need to clarify the orderly allocation and use of `syncrepl` RIDs on all `syncrepl` LDAP slave servers (which will now include special-cased LDAP 'client' machines, as described in 2.2 above.) A posting to the '!OpenLDAP Technical' mailing list suggests that this might be easier than we have thought up till now.

4. Miscellaneous

The hard-coded dependency on a local LDAP server (i.e. a server running on `localhost`) in the `dice-authorize` package (†) noted in the Initial ideas document was addressed in the manner suggested in the final paragraph of Section 3.1.1.1 of that document. Namely: the DICE authorization process now looks up netgroups via the `/etc/nsswitch.conf` configuration, rather than making explicit LDAP lookups for 'capabilities' data. Refer to LCFG Bug #792 for more information, and for references to historical context which might otherwise be lost.

No other hard-coded dependencies on local LDAP servers were uncovered within DICE in the course of the work and testing associated with this project. If any such are subsequently discovered, then they will need to be dealt with as appropriate.

(† The `dice-authorize` package - or its current replacement - is used to authorize access rights within the `om` command.)

5. Effort

The total effort for this work is approximately 30 days. That includes orientation,

prototyping, testing, the establishment of the currently-running test service, and documentation. It also includes work done on the `dice-authorize` package.

6. Lessons learned (?)

1. The initial time allocated for this project was 20 days. That would be unreasonably small amount of time if the aims of the project were expected include a fully completed and operational final implementation, along with the resolution of all details. In the current case, where the final implementation is now coupled into the forthcoming OS upgrade project, precise allocation of work effort and precise time-keeping have become a little difficult. But that is probably inevitable in what started life as a very open 'investigational' project.
2. This project has been running for more than 18 months. Whilst much of the past year has been spent merely 'watching' the test installation in order to be satisfied that it was a viable idea, it's probably a bad idea for *any* project like this to be allowed to continue for so long: at the very least, focus and attention can drift. The 'solution' is probably to subdivide such projects into smaller sub-projects which run to much shorter timescales.

-- IanDurkacz - 11 Dec 2014

This topic: DICE > WebHome > DevelopmentMeeting > FinalProjectReports > FinalProjectReport-267
Topic revision: r5 - 13 Dec 2014 - 10:13:38 - IanDurkacz