Infrastructure - Task #4253

Task # 4246 (In Progress): Determine why cn-stage-ucsb-1 LDAP syncrepl is failing

Build slapd stage cn log event logging into Splunk

2014-02-03 17:55 - David Doyle

Status:	Closed	**Start date:**	2014-02-03
Priority:	Normal	**Due date:**	
Assignee:	David Doyle	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

When the Splunk system was first set up, we removed slapd entries from the logs being sent to Splunk due to debug spam. Unfortunately, this gets rid of the events we need to figure out the ldap sync issue. Need to send these events into their own index in Splunk.

History

#1 - 2014-02-10 06:29 - David Doyle

- Status changed from In Progress to Testing

- % Done changed from 0 to 80

Simple fix - changed the last line of /etc/rsyslog.d/30-splunk.conf from

*.debug @@splunk-forwarder-orc-1.dataone.org:29996

to

*.debug @@splunk-forwarder-orc-1.dataone.org:29996

on the stage CNs. This is sending "debug" info (as slapd is currently set up to generate it, which apparently isn't as simple as a "debug" level) to rsyslog, and then on to Splunk. This generates a negligible level of index activity on the Splunk server, given our license level and current index activity.

Will continue testing with Splunk and adjust slapd log behavior further if needed.

#2 - 2014-02-12 17:58 - David Doyle

- % Done changed from 80 to 100

Getting plenty of slapd log data into Splunk. Calling this done - will add more via loglevel tweaks if needed.

#3 - 2014-02-12 17:58 - David Doyle

- translation missing: en.field_remaining_hours set to 0.0

- Status changed from Testing to Closed

#4 - 2014-02-14 17:59 - David Doyle

- Subject changed from Build slapd log event logging into Splunk to Build slapd stage cn log event logging into Splunk

- Estimated time set to 0.00