Infrastructure - Task #7263

Story # 7259 (Closed): A DEV2 development environment is needed for upgrade testing

Install CCI 1.5.x on cn-dev-ucsb-2 and cn-dev-unm-2

2015-07-16 16:52 - Chris Jones

Status:	Closed	**Start date:**	2015-07-16
Priority:	Normal	**Due date:**	
Assignee:	Chris Jones	**% Done:**	100%
Category:	Environment.Development2	**Estimated time:**	0.00 hour
Target version:	CCI-2.0.0		
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

To simulate the upgrade process from 1.5.x to 2.0.0, we need the DEV2 environment to start out as 1.5.x. Install the CN stack at this point. Consider cloning the VM in case we need to roll back to start over while testing the upgrades.

History

#1 - 2015-07-24 17:45 - Chris Jones

- Status changed from New to In Progress

- % Done changed from 0 to 30

I'm running into some installation issues for the dataone-cn-os-core package. See #7271, but after resolving that, installation fails because the dc=dataone,dc=org LDAP tree fails to be installed during the postinst. This may be caused by the fact that the dc=org tree also didn't get installed, but the postinst test doesn't seem to indicate a failure. Need to check into why, but I've installed them manually in order to continue.

#2 - 2015-07-26 22:33 - Chris Jones

- Status changed from In Progress to Closed

- % Done changed from 30 to 100

- translation missing: en.field_remaining_hours set to 0.0

After running into an issue inserting the object format list:

<?xml version="1.0"?>

schema_reference.4: Failed to read schema document 'https://cn-dev-ucsb-2.test.dataone.org:443/metacat/schema/dataone/dataoneTypes.xsd', because 1) could not find the document; 2) the document could not be read; 3) the root element of the document is not xsd:schema.

Ben pointed out it may be a CA certificate issue. Dave recently updated the wildcard certs to use SHA256, and the GeoTrust intermediate certs were also updated. The CCI 1.5.2 tagged version don't include this new intermediate cert, so I had to manually install it in /etc/ssl/certs and in the cacerts keystore.