Infrastructure - Story #2468

Change how we use certificates in the CN

2012-03-10 02:25 - Robert Waltz

Status:	Closed	**Start date:**	2012-03-10
Priority:	High	**Due date:**	
Assignee:	Ben Leinfelder	**% Done:**	100%
Category:	d1_cn_buildout	**Estimated time:**	0.00 hour
Target version:	Sprint-2012.17-Block.3.1		
Story Points:			

Description

We will have two certificate files. One for use with D1Client, the other for use with Metacat replication.

The one for use with D1Client will become the subject of the CN in the nodelist.

They will both be stored in /etc/dataone/client/certs

during postinst of dataone-cn-os-core, they should both be shown during certificate selection time. But the correct one should be selected (wonder if we can make it a real selection instead of a text box)

The cert selected in dataone-cn-os-core postinst will become named in node.properties.

A similar process should be used for metacat...

Maybe we should just create a /etc/dataone/metacat directory and place the cert in there. Make it a lot easier for automated installs.

We have public keys published, and private keys elsewhere. We need them combined into the same pem for d1Client to interact.

combining them is not so important for metacat.

History

#1 - 2012-03-16 02:32 - Dave Vieglais

- Target version changed from Sprint-2012.09-Block.2.1 to Sprint-2012.11-Block.2.2

- Position set to 13

#2 - 2012-04-23 17:04 - Dave Vieglais

- Assignee changed from Robert Waltz to Chris Jones

- Target version changed from Sprint-2012.11-Block.2.2 to Sprint-2012.17-Block.3.1

#3 - 2012-04-25 23:48 - Ben Leinfelder

- Assignee changed from Chris Jones to Ben Leinfelder

#4 - 2012-05-03 23:41 - Ben Leinfelder

- Status changed from New to Closed

There are now prompts for the Metacat certificate, private key, and optional key password during dataone-cn-metacat configuration. This is independent from the dataone-cn-os-core configuration that prompts for a single .pem that includes the dataone client certificate and private key in the single file.
for cn-dev* I've opted for these locations:

/etc/dataone/client/private/ -- contains the private key used by Metacat replication
/etc/dataone/client/certs/ -- contains both the Metacat replication certificate and also the combined DataONE-issued certifcate/privatekey pem file

Also, cn-buildout is now using the new DataONETestCA so all future deployments should use this CA or the final production CA when we get around to that.