

EOS - Bug #10760

Update test EOS certificates to CILogon

11/03/2015 04:22 PM - Gerard Bernabeu Altayo

Status:	Resolved	Start date:	11/03/2015
Priority:	Normal	Due date:	11/30/2015
Assignee:	Gerard Bernabeu Altayo	% Done:	0%
Category:		Estimated time:	16.00 hours
Target version:		Spent time:	0.00 hour
Description			
I need to update the test instance of EOS to get a new CILogon certificate and test that both gridftp and bestman work.			
Contact Neha for further instructions on how to get a cert.			

History

#1 - 11/05/2015 10:40 AM - Gerard Bernabeu Altayo

Obtaining certs

If needed, certs can be obtained via

User - <https://oim-itb.grid.iu.edu/oim/certificaterequestuser>

Host/Service - <https://oim-itb.grid.iu.edu/oim/certificaterequesthost>

Please let me know if you have any related questions/concerns.

#2 - 11/30/2015 01:48 PM - Gerard Bernabeu Altayo

I've requested 2 certs:

```
[root@cmsstor150 ~]# umask 077; openssl req -new -newkey rsa:2048 -nodes -keyout hostkey.pem -subj "/CN=`hostname --fqdn`"
```

and

```
[root@cmssrv151 grid-security]# umask 077; openssl req -new -newkey rsa:2048 -nodes -keyout cmseoskey-cilogon.pem -subj "/CN=cmssrv152.fnal.gov"
```

#3 - 12/01/2015 04:25 PM - Gerard Bernabeu Altayo

Certificates downloaded and added in the secret repo certs:

```
mac-124183:Downloads gerard1$ scp host_certificate.H6486.cmsstor150.fnal.gov.x509.pem root@cmsadmin1.fnal.gov
:/srv/secrets/cmsstor150.fnal.gov/hostcert.pem
host_certificate.H6486.cmsstor150.fnal.gov.x509.pem 100% 1532 1.5KB/s 00:00
mac-124183:Downloads gerard1$ scp host_certificate.H6487.cmssrv152.fnal.gov.x509.pem root@cmsadmin1.fnal.gov
:/srv/secrets/cmssrv152.fnal.gov/hostcert.pem
host_certificate.H6487.cmssrv152.fnal.gov.x509.pem 100% 1528 1.5KB/s 00:00
mac-124183:Downloads gerard1$
```

And moving the keys there too:

```
[root@cmsstor150 ~]# scp hostkey.pem root@cmsadmin1.fnal.gov:/srv/secrets/cmsstor150.fnal.gov/
hostkey.pem 100% 1704 1.7KB/s 00:00
[root@cmsstor150 ~]#
[root@cmssrv151 grid-security]# scp cmseoskey-cmssrv152-cilogon.pem root@cmsadmin1.fnal.gov:/srv/secrets/cmssrv152.fnal.gov/hostkey.pem
cmseoskey-cmssrv152-cilogon.pem 100% 1704 1.7KB/s 00:00
[root@cmssrv151 grid-security]#
```

Lisa pushed some of my changes at the same time while I was doing this so to see the actual changes I'm making something a bit funny:

```
[root@cmsadmin1 secrets]# git diff --name-status f51a18aa179f967ac6af30103343be50bddb72a6 | grep -v cmseos
M cmssrv152.fnal.gov/hostcert.pem
A cmssrv152.fnal.gov/hostcert.pem.old
M cmssrv152.fnal.gov/hostkey.pem
A cmssrv152.fnal.gov/hostkey.pem.old
M cmsstor150.fnal.gov/hostcert.pem
A cmsstor150.fnal.gov/hostcert.pem.old
M cmsstor150.fnal.gov/hostkey.pem
```

```
A cmsstor150.fnal.gov/hostkey.pem.old
[root@cmsadmin1 secrets]#
```

Now I'll use puppet to roll this out. Note that I don't fully remember the status of puppet deployment for this certs so I may have to do something additional...

#4 - 12/08/2015 04:44 PM - Gerard Bernabeu Altayo

First trying to get the certs pushed out to cmssrv151:

```
[root@cmssrv151 grid-security]# mkdir oldcerts
[root@cmssrv151 grid-security]# ll *.pem*
-rw-r--r-- 1 root root 2022 Apr 27 2015 cmseoscert.pem
-rw----- 1 root root 1704 Nov 30 13:44 cmseoskey-cmssrv152-cilogon.pem
-r----- 1 root root 1675 Apr 27 2015 cmseoskey.pem
-rw-r--r-- 1 root root 2022 Jan 20 2015 hostcert.pem
-rw-r--r-- 1 root root 2022 Dec 10 2013 hostcert.pem.OLD
-r----- 1 root root 1675 Jan 20 2015 hostkey.pem
-r----- 1 root root 1679 Dec 10 2013 hostkey.pem.OLD
[root@cmssrv151 grid-security]# mv *.pem* oldcerts/
[root@cmssrv151 grid-security]# ll
total 408
drwxr-xr-x 2 daemon daemon 4096 Jun 24 12:17 bestman
drwxr-xr-x 2 daemon daemon 4096 Apr 27 2015 bestman2
lrwxrwxrwx 1 root root 20 Nov 3 18:44 certificates -> certificates-1.50NEW
drwxr-xr-x 2 root root 53248 Oct 13 14:24 certificates-1.49NEW.old
drwxr-xr-x 2 root root 53248 Nov 3 18:48 certificates-1.50NEW
drwxr-xr-x 2 daemon daemon 4096 Jun 24 12:15 daemon
-rw-r--r-- 1 root root 278535 Dec 8 13:15 grid-mapfile
drwxr-xr-x 2 root root 4096 Dec 8 16:39 oldcerts
drwxr-xr-x 2 root root 4096 Apr 28 2015 vommdir
[root@cmssrv151 grid-security]# ll bestman*
bestman:
total 8
-rw-r--r-- 1 bestman bestman 2022 Jun 24 12:17 bestmancert.pem
-r----- 1 bestman bestman 1679 Jun 24 12:15 bestmankey.pem

bestman2:
total 0
lrwxrwxrwx 1 daemon daemon 42 Apr 27 2015 hostcert.pem -> /etc/grid-security/bestman/bestmancert.pem
lrwxrwxrwx 1 daemon daemon 41 Apr 27 2015 hostkey.pem -> /etc/grid-security/bestman/bestmankey.pem
[root@cmssrv151 grid-security]# mv bestman oldcerts/
[root@cmssrv151 grid-security]# puppet agent -t
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts in /var/lib/puppet/lib/facter/afs_cache_size.rb
Info: Loading facts in /var/lib/puppet/lib/facter/os_maj_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/cvmfspartsize.rb
Info: Loading facts in /var/lib/puppet/lib/facter/facter_dot_d.rb
Info: Loading facts in /var/lib/puppet/lib/facter/iptables_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/pe_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/concat_basedir.rb
Info: Loading facts in /var/lib/puppet/lib/facter/condorceversion.rb
Info: Loading facts in /var/lib/puppet/lib/facter/postgres_default_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/rsyslog_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/code_server.rb
Info: Loading facts in /var/lib/puppet/lib/facter/root_home.rb
Info: Loading facts in /var/lib/puppet/lib/facter/iptables_persistent_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/certificate_facts.rb
Info: Loading facts in /var/lib/puppet/lib/facter/puppet_vardir.rb
Info: Loading facts in /var/lib/puppet/lib/facter/ip6tables_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/cvmfsversion.rb
Info: Caching catalog for cmssrv151.fnal.gov
Info: Applying configuration version '1449614349'
Notice: /Stage[main]/P_grid_certificate/P_secret::File[/etc/grid-security/hostkey.pem]/File[/etc/grid-security/hostkey.pem]/ensure: defined content as '{md5}0369b0729d286401e87d65692f9a0e39'
Notice: /Stage[main]/P_grid_certificate/P_secret::File[/etc/grid-security/hostcert.pem]/File[/etc/grid-security/hostcert.pem]/ensure: defined content as '{md5}522248c471a406067757922a0c9b24ea'
Notice: /Stage[main]/Eos::Gridcerts/File[/etc/grid-security/bestman]/ensure: created
Notice: /Stage[main]/Eos::Gridcerts/File[/etc/grid-security/bestman/bestmancert.pem]/ensure: defined content as '{md5}b846148aelca7ab7b0ab2129e8795526'
Notice: /Stage[main]/Eos::Gridcerts/File[/etc/grid-security/bestman/bestmankey.pem]/ensure: defined content as '{md5}43e3a9b564ef528c7109233254abca00'
Notice: Finished catalog run in 25.78 seconds
[root@cmssrv151 grid-security]#
```

Checking the deployed certs:

```
[root@cmsrv151 grid-security]# openssl x509 -noout -text -in /etc/grid-security/hostcert.pem | grep Subject:
    Subject: DC=com, DC=DigiCert-Grid, O=Open Science Grid, OU=Services, CN=cmsrv151.fnal.gov
[root@cmsrv151 grid-security]#
[root@cmsrv151 grid-security]# openssl x509 -noout -text -in /etc/grid-security/bestman/bestmancert.pem | gre
p Subject:
    Subject: DC=com, DC=DigiCert-Grid, O=Open Science Grid, OU=Services, CN=cmsrv152.fnal.gov
[root@cmsrv151 grid-security]#
```

So.. Failure, the proper certs have not been pushed!

Ups... I had to do this on cmsrv153! Going for that.

#5 - 12/08/2015 05:48 PM - Gerard Bernabeu Altayo

Checking on the (simpler) FST node cmsstor150.

The cert here was deployed a week ago, when I pushed it to the secrets repo:

```
[root@cmsstor150 ~]# ls -ltrah /etc/grid-security/
total 412K
drwxr-xr-x    2 root root   52K Oct 14 08:47 certificates-1.49NEW.old
lrwxrwxrwx    1 root root    20 Nov  3 17:14 certificates -> certificates-1.50NEW
drwxr-xr-x    2 root root   52K Nov  3 18:43 certificates-1.50NEW
-r-----    1 root root   1.7K Dec  1 17:02 hostkey.pem
-rw-r--r--    1 root root   1.5K Dec  1 17:02 hostcert.pem
drwxr-xr-x. 110 root root   12K Dec  3 03:29 ..
-rw-r--r--    1 root root  273K Dec  8 13:15 grid-mapfile
drwxr-xr-x.   4 root root   4.0K Dec  8 13:15 .
[root@cmsstor150 ~]# openssl x509 -noout -text -in /etc/grid-security/hostcert.pem | grep Subject:
    Subject: DC=org, DC=opensciencegrid, O=Open Science Grid, OU=Services, CN=cmsstor150.fnal.gov
[root@cmsstor150 ~]# openssl x509 -noout -text -in /etc/grid-security/hostcert.pem | grep Issuer:
    Issuer: DC=org, DC=cilogon, C=US, O=CILogon, CN=CILogon OSG CA 1
```

On the other headnode the change didn't work very well either:

```
[root@cmsrv153 grid-security]# openssl x509 -noout -text -in /etc/grid-security/bestman/bestmancert.pem | gre
p Subject:
    Subject: DC=com, DC=DigiCert-Grid, O=Open Science Grid, OU=Services, CN=cmsrv152.fnal.gov
[root@cmsrv153 grid-security]# openssl x509 -noout -text -in /etc/grid-security/hostcert.pem | grep Subject:
    Subject: DC=com, DC=DigiCert-Grid, O=Open Science Grid, OU=Services, CN=cmsrv153.fnal.gov
[root@cmsrv153 grid-security]#
```

I will test to check if the current gridftp transfer works at least, going to an (old digicert) bestman but to a CILogon gridftp server.... It's a good test because apparently this never worked! The poor test bestman is setup thinking it's the production one, see error:

```
[srminfo]Unrecognizable url:srm://cmsrv152.fnal.gov:8443/srm/v2/server?SFN=/eos/cmseos-test.fnal.gov/data/ger
ard/bin.tar for this server:httpg://cmseos.fnal.gov:8443/srm/v2/server
```

This is on cmsrv153 when trying the following from cmsphedex-disk as cmsprod:

```
-bash-4.1$ export X509_USER_PROXY=/home/cmsprod/phedex/gridcert/proxy.cert
-bash-4.1$ srmcp -debug -2 srm://cmsrv152.fnal.gov:8443/srm/v2/server?SFN=/eos/cmseos-test.fnal.gov/data/ger
ard/bin.tar file:///tmp/test.gba
```

After a decent amount of bug-fixing and hackery now this works:

```
-bash-4.1$ srmcp -debug -2 srm://cmsrv152.fnal.gov:8443/srm/v2/server?SFN=/eos/test/gba.test.touch file:///t
mp/test.gba.$$
```

```
-bash-4.1$ globus-url-copy -dbg gsiftp://cmsstor150.fnal.gov//eos/test/gba.test.touch file:///home/cmsprod/m
yfile.test.gba.gftp
```

All the hackery is done manual, with puppet disabled, on cmsrv153 (EOS MGM and bestman server), need to puppetize it all:

1. Add cmsstor150.fnal.gov in the list of 'unix' authorized hosts in /etc/xrd.cf.mgm
2. change /etc/bestman2/conf/bestman2.rc so that

```
[root@cmsrv153 grid-security]# grep cmsrv152 /etc/sysconfig/bestman2 /etc/bestman2/conf/bestman2.rc
/etc/sysconfig/bestman2:GLOBUS_HOSTNAME=cmsrv152.fnal.gov
/etc/bestman2/conf/bestman2.rc:supportedProtocolList=gsiftp://cmsstor150.fnal.gov;srm://cmseos-test.fnal.gov;s
```

```
rm://cmssrv152.fnal.gov;srm://cmssrv153.fnal.gov;srm://cmssrv151.fnal.gov
```

```
#AND
```

```
localPathListAllowed=/eos/uscms;/lustre/unmerged;/eos/test
```

3. Actually I should stop using cmssrv152 and get cmseos-test.fnal.gov on (need to get cert, the ip is already there!).

#6 - 12/08/2015 05:54 PM - Gerard Bernabeu Altayo

- Status changed from New to Resolved

Doing a quick&dirty test to get the CILogon certs in place:

```
[root@cmssrv153 bestman]# ll
total 8
-rw-r--r-- 1 bestman bestman 2022 Dec  8 16:44 bestmancert.pem
-r----- 1 bestman bestman 1679 Dec  8 16:44 bestmankey.pem
[root@cmssrv153 bestman]# scp root@cmsadmin1.fnal.gov:/srv/secrets/cmssrv152.fnal.gov/hostkey.pem bestmankey.p
em
hostkey.pem
                                100% 1704    1.7KB/s   00:00
[root@cmssrv153 bestman]# scp root@cmsadmin1.fnal.gov:/srv/secrets/cmssrv152.fnal.gov/hostcert.pem bestmancert
.pem
hostcert.pem
                                100% 1528    1.5KB/s   00:00
[root@cmssrv153 bestman]# ll
total 8
-rw-r--r-- 1 bestman bestman 1528 Dec  8 17:49 bestmancert.pem
-r----- 1 bestman bestman 1704 Dec  8 17:49 bestmankey.pem
[root@cmssrv153 bestman]# cd ..
[root@cmssrv153 grid-security]# ll
total 416
drwxr-xr-x 2 daemon daemon  4096 Dec  8 16:44 bestman
drwxr-xr-x 2 daemon daemon  4096 Apr 27  2015 bestman2
lrwxrwxrwx 1 root   root    20 Dec  8 14:22 certificates -> certificates-1.51NEW
drwxr-xr-x 2 root   root   53248 Nov  3 18:48 certificates-1.50NEW.old
drwxr-xr-x 2 root   root   53248 Dec  8 14:22 certificates-1.51NEW
drwxr-xr-x 2 daemon daemon  4096 Jun 24 12:16 daemon
-rw-r--r-- 1 root   root  278535 Dec  8 13:08 grid-mapfile
-rw-r--r-- 1 root   root   2022 Dec  8 16:44 hostcert.pem
-r----- 1 root   root   1675 Dec  8 16:44 hostkey.pem
drwxr-xr-x 3 root   root   4096 Dec  8 16:44 oldcerts
drwxr-xr-x 2 root   root   4096 Apr 28  2015 vommdir
[root@cmssrv153 grid-security]# rm -f hostcert.pem hostkey.pem
[root@cmssrv153 grid-security]# service bestman2 restart
Shutting down bestman2:                                [ OK ]
Starting bestman2:                                     [ OK ]
[root@cmssrv153 grid-security]#
[root@cmssrv153 grid-security]# openssl x509 -noout -text -in /etc/grid-security/bestman/bestmancert.pem | gre
p Subject:
    Subject: DC=org, DC=open-science-grid, O=Open Science Grid, OU=Services, CN=cmssrv152.fnal.gov
[root@cmssrv153 grid-security]# openssl x509 -noout -text -in /etc/grid-security/bestman/bestmancert.pem | gre
p Issuer:
    Issuer: DC=org, DC=cilogon, C=US, O=CILogon, CN=CILogon OSG CA 1
[root@cmssrv153 grid-security]#
```

Tested a transfer and it worked! Sending email to Neha about it.