

## Infrastructure - Bug #8788

### LE(?) certs not installed with the correct permissions on cn-dev-orc-1

2019-04-30 16:56 - Rob Nahf

<b>Status:</b>	Closed	<b>Start date:</b>	2019-04-30
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Dave Vieglais	<b>% Done:</b>	100%
<b>Category:</b>	Support Operations	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>		<b>Story Points:</b>	
<b>Milestone:</b>	None		
<b>Product Version:</b>	*		

#### Description

when installing dataone-cn-metacat and dataone-cn-index, postinst returned errors from incorrect permissions in the LE certificate. These were installed only 2 weeks ago, so I assume the issue is with the certificate installation process, not something to do with the dataone packages.

the exception was:

```
2019-04-28 23:32:06 UTC FATAL: private key file "/var/lib/postgresql/9.3/main/server.key" has group or world access
2019-04-28 23:32:06 UTC DETAIL: File must have permissions u=rw (0600) or less if owned by the database user, or permissions u=rw,g=r (0640) or less if owned by root.
```

permissions on the file (privkey5.pem) were:

```
-rw-r----- 1 root ssl-cert 1704 Aug 17 2018 privkey1.pem
-rw-r----- 1 root ssl-cert 1704 Oct 17 2018 privkey2.pem
-rw-r----- 1 root ssl-cert 1704 Dec 16 12:33 privkey3.pem
-rw-r----- 1 root ssl-cert 1704 Feb 14 12:21 privkey4.pem
-rw-r--r-- 1 root root 1704 Apr 15 12:50 privkey5.pem
```

#### History

##### #1 - 2019-04-30 16:57 - Rob Nahf

- Description updated

##### #2 - 2019-05-21 12:51 - Dave Vieglais

After the lets encrypt certs are updated, it is necessary to run a script to set permissions consistently across the CNs. This is done by the script /etc/letsencrypt/post-cn-renewal.sh

##### #3 - 2019-05-21 12:51 - Dave Vieglais

- % Done changed from 0 to 100
- Assignee set to Dave Vieglais
- Status changed from New to Closed