hswaw - Bugless #36

k0: refresh certificates

03/27/2021 11:28 AM - q3k

Status:	Resolved
Priority:	Normal
Assignee:	q3k
Category:	

Description

Some certs expire tomorrow:

```
$ for f in cluster/certs/*c*rt; do echo -n $f; openssl x509 -text < $f | grep After; done | grep 2
021 | grep Mar | column -t
cluster/certs/etcd-bc01n01.hswaw.net.cert          Not  After  :  Mar  28  15:53:00  2021  GMT
cluster/certs/etcd-bc01n02.hswaw.net.cert          Not  After  :  Mar  28  16:45:00  2021  GMT
cluster/certs/etcd-bc01n03.hswaw.net.cert          Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/etcd-calico.cert                     Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/etcd-kube.cert                       Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/etcdpeer-bc01n01.hswaw.net.cert      Not  After  :  Mar  28  15:53:00  2021  GMT
cluster/certs/etcdpeer-bc01n02.hswaw.net.cert      Not  After  :  Mar  28  16:45:00  2021  GMT
cluster/certs/etcdpeer-bc01n03.hswaw.net.cert      Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/etcd-root.cert                       Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/kube-controllermanager.cert          Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/kubefront-apiserver.cert             Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/kube-kubelet-bc01n01.hswaw.net.cert  Not  After  :  Mar  28  15:53:00  2021  GMT
cluster/certs/kube-kubelet-bc01n02.hswaw.net.cert  Not  After  :  Mar  28  16:45:00  2021  GMT
cluster/certs/kube-kubelet-bc01n03.hswaw.net.cert  Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/kube-proxy.cert                      Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/kube-scheduler.cert                  Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/kube-serviceaccounts.cert            Not  After  :  Mar  28  15:15:00  2021  GMT
```

History

#1 - 03/27/2021 11:29 AM - q3k

- Description updated

- Status changed from New to Accepted

- Assignee set to q3k

#2 - 03/27/2021 11:33 AM - q3k

Starting off with `bazel run //cluster/clustercfg -- nodestrap bc01n01`:

```
INFO - Nodestrapping bc01n01.hswaw.net...
INFO - etcdpeer-bc01n01.hswaw.net: Renewing certificate...
INFO - Decrypting etcdpeer-bc01n01.hswaw.net.key (/home/q3k/hscloud/cluster/secrets/cipher/etcdpeer-bc01n01.hs
waw.net.key)...
INFO - CN=etcd peer ca (etcdpeer): Generating CSR for ['bc01n01.hswaw.net']
INFO - CN=etcd peer ca (etcdpeer): Signing CSR
INFO - Decrypting ca-etcdpeer.key (/home/q3k/hscloud/cluster/secrets/cipher/ca-etcdpeer.key)...
INFO - CN=etcd peer ca (etcdpeer): Saving new certificate to /home/q3k/hscloud/cluster/certs/etcdpeer-bc01n01.
hswaw.net.cert
INFO - etcd-bc01n01.hswaw.net: Renewing certificate...
INFO - Decrypting etcd-bc01n01.hswaw.net.key (/home/q3k/hscloud/cluster/secrets/cipher/etcd-bc01n01.hswaw.net.
key)...
INFO - CN=etcd ca (etcd): Generating CSR for ['bc01n01.hswaw.net']
INFO - CN=etcd ca (etcd): Signing CSR
INFO - Decrypting ca-etcd.key (/home/q3k/hscloud/cluster/secrets/cipher/ca-etcd.key)...
INFO - CN=etcd ca (etcd): Saving new certificate to /home/q3k/hscloud/cluster/certs/etcd-bc01n01.hswaw.net.cer
t
INFO - etcd-kube: Renewing certificate...
INFO - Decrypting etcd-kube.key (/home/q3k/hscloud/cluster/secrets/cipher/etcd-kube.key)...
INFO - CN=etcd ca (etcd): Generating CSR for ['kube']
INFO - CN=etcd ca (etcd): Signing CSR
INFO - CN=etcd ca (etcd): Saving new certificate to /home/q3k/hscloud/cluster/certs/etcd-kube.cert
INFO - etcd-root: Renewing certificate...
```

```
INFO - Decrypting etcd-root.key (/home/q3k/hscloud/cluster/secrets/cipher/etcd-root.key)...
INFO - CN=etcd ca (etcd): Generating CSR for ['root']
INFO - CN=etcd ca (etcd): Signing CSR
INFO - CN=etcd ca (etcd): Saving new certificate to /home/q3k/hscloud/cluster/certs/etcd-root.cert
INFO - etcd-calico: Renewing certificate...
INFO - Decrypting etcd-calico.key (/home/q3k/hscloud/cluster/secrets/cipher/etcd-calico.key)...
INFO - CN=etcd ca (etcd): Generating CSR for ['calico']
INFO - CN=etcd ca (etcd): Signing CSR
INFO - CN=etcd ca (etcd): Saving new certificate to /home/q3k/hscloud/cluster/certs/etcd-calico.cert
INFO - kube-kubelet-bc01n01.hswaw.net: Renewing certificate...
INFO - Decrypting kube-kubelet-bc01n01.hswaw.net.key (/home/q3k/hscloud/cluster/secrets/cipher/kube-kubelet-bc
01n01.hswaw.net.key)...
INFO - CN=kubernetes main CA (kube): Generating CSR for ['system:node:bc01n01.hswaw.net', 'bc01n01.hswaw.net']
INFO - CN=kubernetes main CA (kube): Signing CSR
INFO - Decrypting ca-kube.key (/home/q3k/hscloud/cluster/secrets/cipher/ca-kube.key)...
INFO - CN=kubernetes main CA (kube): Saving new certificate to /home/q3k/hscloud/cluster/certs/kube-kubelet-bc
01n01.hswaw.net.cert
INFO - kube-serviceaccounts: Renewing certificate...
INFO - Decrypting kube-serviceaccounts.key (/home/q3k/hscloud/cluster/secrets/cipher/kube-serviceaccounts.key)
...
INFO - CN=kubernetes main CA (kube): Generating CSR for ['serviceaccounts']
INFO - CN=kubernetes main CA (kube): Signing CSR
INFO - CN=kubernetes main CA (kube): Saving new certificate to /home/q3k/hscloud/cluster/certs/kube-serviceacc
ounts.cert
INFO - kube-controllermanager: Renewing certificate...
INFO - Decrypting kube-controllermanager.key (/home/q3k/hscloud/cluster/secrets/cipher/kube-controllermanager.
key)...
INFO - CN=kubernetes main CA (kube): Generating CSR for ['system:kube-controller-manager']
INFO - CN=kubernetes main CA (kube): Signing CSR
INFO - CN=kubernetes main CA (kube): Saving new certificate to /home/q3k/hscloud/cluster/certs/kube-controller
manager.cert
INFO - kube-scheduler: Renewing certificate...
INFO - Decrypting kube-scheduler.key (/home/q3k/hscloud/cluster/secrets/cipher/kube-scheduler.key)...
INFO - CN=kubernetes main CA (kube): Generating CSR for ['system:kube-scheduler']
INFO - CN=kubernetes main CA (kube): Signing CSR
INFO - CN=kubernetes main CA (kube): Saving new certificate to /home/q3k/hscloud/cluster/certs/kube-scheduler.
cert
INFO - kube-proxy: Renewing certificate...
INFO - Decrypting kube-proxy.key (/home/q3k/hscloud/cluster/secrets/cipher/kube-proxy.key)...
INFO - CN=kubernetes main CA (kube): Generating CSR for ['system:kube-proxy']
INFO - CN=kubernetes main CA (kube): Signing CSR
INFO - CN=kubernetes main CA (kube): Saving new certificate to /home/q3k/hscloud/cluster/certs/kube-proxy.cert
INFO - kubefront-apiserver: Renewing certificate...
INFO - Decrypting kubefront-apiserver.key (/home/q3k/hscloud/cluster/secrets/cipher/kubefront-apiserver.key)..
.
INFO - CN=kubernetes frontend CA (kubefront): Generating CSR for ['apiserver']
INFO - CN=kubernetes frontend CA (kubefront): Signing CSR
INFO - Decrypting ca-kubefront.key (/home/q3k/hscloud/cluster/secrets/cipher/ca-kubefront.key)...
INFO - CN=kubernetes frontend CA (kubefront): Saving new certificate to /home/q3k/hscloud/cluster/certs/kubefr
ont-apiserver.cert
```

#3 - 03/27/2021 11:38 AM - q3k

Rolled out to bc01n01:

```
[...]
would stop the following units: etcd.service, kube-apiserver.service, kube-controller-manager.service, kube-pr
oxy.service, kube-scheduler.service, kubelet.service
would start the following units: etcd.service, kube-apiserver.service, kube-controller-manager.service, kube-p
roxy.service, kube-scheduler.service, kubelet.service
Do you want to switch to this configuration? y
updating GRUB 2 menu...
stopping the following units: etcd.service, kube-apiserver.service, kube-controller-manager.service, kube-prox
y.service, kube-scheduler.service, kubelet.service
activating the configuration...
setting up /etc...
reloading user units for root...
setting up tmpfiles
starting the following units: etcd.service, kube-apiserver.service, kube-controller-manager.service, kube-prox
y.service, kube-scheduler.service, kubelet.service
the following new units were started: session-7.scope

$ kubectl get nodes
NAME                 STATUS   ROLES    AGE     VERSION
bc01n01.hswaw.net    Ready    &lt;none&gt;   2y69d   v1.16.6-beta.0
```

```
bc01n02.hswaw.net    Ready    &lt;none&gt;   2y74d   v1.16.6-beta.0
dcr01s22.hswaw.net   Ready    &lt;none&gt;   512d    v1.16.6-beta.0
dcr01s24.hswaw.net   Ready    &lt;none&gt;   512d    v1.16.6-beta.0
```

Draining seemed not necessary, likely continiuing drainless restarts for rest of nodes.

#4 - 03/27/2021 11:43 AM - q3k

Rolled out to bc01n02.

#5 - 03/27/2021 11:48 AM - q3k

Rolled out dcr01s22.hswaw.net.

#6 - 03/27/2021 11:49 AM - q3k

Rolled out dcr01s24.hswaw.net.

#7 - 03/27/2021 11:50 AM - q3k

Cluster seems healthy.

Cert files still expiring soon in Git are ones for the decomissioned bc01n03:

```
cluster/certs/etcd-bc01n03.hswaw.net.cert          Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/etcdpeer-bc01n03.hswaw.net.cert      Not  After  :  Mar  28  15:15:00  2021  GMT
cluster/certs/kube-kubelet-bc01n03.hswaw.net.cert  Not  After  :  Mar  28  15:15:00  2021  GMT
```

Deleting them alongside their respective private keys.

Next step: ensure certs within k0 objects are updated.

#8 - 03/27/2021 11:58 AM - q3k

Only k0 object affected seems to be the calico-secrets secret in kube-system.

Updated it, now restarting affected calico services.

#9 - 03/27/2021 12:03 PM - q3k

That secret is used by calico-node and calico-kbue-controllers pods.

```
$ kubectl -n kube-system get pods -o wide | grep calico
calico-kube-controllers-67b8b986cc-bgtsc   1/1     Running   1          41d    185.236.240.39   dcr01s22.hswaw
.net   &lt;none&gt;           &lt;none&gt;
calico-node-8xtss                          1/1     Running   1          167d   185.236.240.35   bc01n01.hswaw.
net    &lt;none&gt;           &lt;none&gt;
calico-node-hxllk                          1/1     Running   1          174d   185.236.240.40   dcr01s24.hswaw
.net   &lt;none&gt;           &lt;none&gt;
calico-node-s8skk                          1/1     Running   1          167d   185.236.240.36   bc01n02.hswaw.
net    &lt;none&gt;           &lt;none&gt;
calico-node-sp66m                          1/1     Running   1          101d   185.236.240.39   dcr01s22.hswaw
.net   &lt;none&gt;           &lt;none&gt;
```

Restarting:

```
$ kubectl -n kube-system delete pod calico-node-8xtss # bc01n01 daemon
$ kubectl -n kube-system get pods -o wide | grep calico | grep bc01n01
calico-node-q654l                          1/1     Running   0          23s    185.236.240.35   bc01n01.hswaw.
net    &lt;none&gt;           &lt;none&gt;
```

Came back up. Restarting rest to ensure they load the new certs, including controller.

#10 - 03/27/2021 12:05 PM - q3k

Looks like dcr01s22 still has a calico/kube node misconfiguration issue:

```
2021-03-27 12:03:54.958 [WARNING][9] startup/startup.go 1203: Failed to set NetworkUnavailable to False; will
retry error=nodes "dcr01s22" not found
```

This slows up startup, but it does end up becoming healthy. It's the same thing for dcr01s24. I vaguely remember attempting to fix that at some point, but probably gave up because the constant network restarts were not worth it.

#11 - 03/27/2021 12:10 PM - q3k

Calico restarted, including controller.

Controller complains about not being able to connect to bc01n03:

```
W0327 12:10:27.584455       1 clientconn.go:1120] grpc: addrConn.createTransport failed to connect to {https:/
/bc01n03.hswaw.net:2379 0  &lt;nil&gt;}. Err :connection error: desc = "transport: Error while dialing dial tc
p 185.236.240.37:2379: connect: no route to host". Reconnecting...
```

We should probably fix that.

#12 - 03/27/2021 12:14 PM - q3k

Filed #38 and #39 for calico deployment issues.

Filing CRs for cert updates in git.

#13 - 03/27/2021 12:20 PM - q3k

- Status changed from Accepted to Resolved

Merged cr/885 and cr/887. Followup refresh in #40.

All done.