（New in v1.1） CockroachDB允许用户在不重启节点的情况下替换安全证书。

**TIPS:** 关于CockroachDB如何在安全模式的集群下进行安全验证，可查阅文档：[创建安全证书](http://doc.cockroachchina.baidu.com/" \l "deploy/create-security-certificates/)

适用场景

* 节点、客户端、CA证书即将过期
* 用户组织规定需要周期性变更证书
* 密钥文件安全无法保障
* 需要修改验证内容，例如添加新的DNS或是负载均衡器的地址，保证其能访问到集群节点。

替换客户端证书

* 创建新的客户端证书和密钥

cockroach cert create-client <username> --certs-**dir**=certs --**ca**-key=my-safe-directory/**ca**.key

* 适用任意方式上传证书和密钥文件到客户端程序所在的机器
* 依据用户不同的应用程序选择相应的方式，来应用新的客户端证书。

替换节点证书

* 创建新的节点证书和密钥

cockroach cert create-node <node hostname> <node other hostname> <node yet another hostname> --certs-dir=certs --ca-key=my-safe-directory/ca.key --overwrite

如果--certs-dir指定的文件夹路径下已经存在老的证书和密钥文件，则需要适用--overwriteFlag覆盖旧文件。

* 上传到节点所在机器上

scp certs/node.crt certs/node.key <username>@<node address>:~/certs

* 重新加载节点证书时无须重启cockroach进程，可以发送SIGHUP信号到cockroach进程：

pkill -SIGHUP -x cockroach

* 在Admin界面中查看**Local Node Certificates**页（https://<address of node with new certs>:8080/#/reports/certificates/local），通过查看验证文件的过期时间是否更新，确认新验证是否成功应用。

替换CA证书

若用户需要替换CA证书，则需要创建新CA密钥并合并CA证书（包含新CA证书和旧CA证书），然后在节点和客户端上重新加载新的CA证书组合。 一旦所有节点和客户端都配置了CA证书组合，用户可以使用新CA证书签名节点和客户端新的证书，再在节点和客户端上重新加载对应的新证书。

配置步骤

* 重命名旧CA证书

mv my-safe-directory/ca.key my-safe-directory/ca.old.key

* 创建新的CA证书和密钥

cockroach cert create-ca --certs-dir=certs --ca-key=my-safe-directory/ca.key --overwrite

此时用户获得了CA证书组合和新的ca.crt文件。

**WARNING:** cockroach命令不会主动加载CA密钥文件，因此需要指定--ca-keyFlag使该文件与其他证书文件存放到不同的位置。

* 上传新的CA证书到每个CockroachDB节点

scp certs/ca.crt

<username>@<node1 address>:~/certs

* 上传新的CA证书到客户端
* 登陆每个CockroachDB节点，为使节点重新加载节点证书，发送SIGHUP信号到cockroach进程：

pkill -SIGHUP -x cockroach

* 依据用户不同的应用程序选择相应的方式，来应用新的CA证书。
* 在Admin界面中查看**Local Node Certificates**页，通过查看CA文件的过期时间是否更新，确认新CA证书是否成功应用。 https://<address of node with new certs>:8080/#/reports/certificates/local
* 在确认集群所有节点成功更新CA证书以后，利用新的CA证书更新节点和客户端的证书。

使用组合CA证书原因

替换CA证书的时候，节点重新扫描指定的certs文件夹，重新加载CA证书。但在使用新CA证书替换客户端和节点证书之前，集群仍然使用旧的CA证书来签名客户端和节点证书，而新CA证书无法验证。

为解决这个问题，CockroachDB需要使用新、旧CA证书合并成组合CA证书，使得节点与客户端的新、旧证书能够分别通过新、旧CA证书得到有效验证。

提前替换CA证书的原因

替换CA证书以后，节点和客户端证书可以使用新的CA证书签名。对于节点来说新CA证书在certs文件夹重新加载以后能够很快应用新CA证书，而对于客户端来说需要重启客户端才能应用新CA证书。未能够及时应用新CA证书的客户端将无法与集群节点成功验证通信。因此为保证集群所有节点和客户端都应用了新CA证书，有必要将CA证书提前替换的过程作为一个完整的阶段。

推荐用户在更新节点和客户端证书之前的几个月提前替换CA证书。