安全模式下的CockroachDB集群，使用[TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security)加密节点之间、节点与客户端之间的通信，需要创建CA证书、节点与客户端的证书和密钥文件。用户可以cockroach cert[命令](http://doc.cockroachchina.baidu.com/#deploy/cockroach-commands/)或者[openssl命令](https://wiki.openssl.org/index.php/)来创建这些验证文件。

**TIPS:** 关于如何在不需要重启节点的情况下修改安全验证方式，可以查看[Rotate Security Certificates](https://www.cockroachlabs.com/docs/stable/rotate-certificates.html)

工作原理

* 执行cockroach cert命令创建CA证书和密钥文件，用于签名节点与客户端的证书。
* 需要上传CA证书到集群的每个节点，并为节点创建节点证书，而客户端则需要创建客户端证书。
* 随后在节点之间、客户端与节点之间创建连接时，需要CA证书验证身份。

Subcommands

| **Subcommand** | **简介** |
| --- | --- |
| create-ca | 创建自签名的CA证书，用于创建和验证集群的其他证书。 |
| create-node | 创建节点的证书和密钥文件，需要通过Flag指定节点所能访问的所有其他节点。 |
| create-client | 创建[指定用户](http://doc.cockroachchina.baidu.com/#deploy/access-management/manage-users/)的证书和密钥文件，用户该用户访问集群节点。 |
| list | 列举出证书目录当中所有的证书和密钥文件。 |

证书目录

使用cockroach cert创建节点和客户端证书时，用户需要使用CA证书和密钥的本地副本。因此，建议在一个位置创建所有证书和密钥，然后分发节点和客户端证书和密钥到适当的集群节点。对于CA密钥文件，**请务必将其存储在安全的位置并保留备份**。如果丢失了CA密钥，将无法向群集添加新节点或客户端。详细的部署流程可以查看[手动部署](http://doc.cockroachchina.baidu.com/#deploy/manual-deployment/overview/)。

create-\*的子命令在--certs-dirFlag指定的目录下创建CA证书、客户端和节点的证书密钥文件，即包括：

| **文件名** | **文件用途** |
| --- | --- |
| ca.crt | CA验证证书 |
| node.crt | 服务端证书 |
| node.key | 服务端证书对应的密钥文件 |
| client.<user>.crt | 用户<user>以客户端访问集群时使用的证书，例如root用户对应 client.root.crt |
| client.<user>.key | 客户端证书对应的密钥文件 |

* cockroach命令不会主动使用CA密钥文件，因此可以使用--ca-keyFlag为其指定单独的存储位置。
* 密钥文件不允许开放除了所有者以外组内其他成员或是其他组的文件权限，即需要设置权限为rwx------。该检查可以通过COCKROACH\_SKIP\_KEY\_PERMISSION\_CHECK=true关闭。

概要

*# Create the CA certificate and key:*

cockroach cert create-ca \

--certs-dir=[path-to-certs-directory] \

--ca-key=[path-to-ca-key]

*# Create a node certificate and key:*

cockroach cert create-node \

[node-hostname] \

[node-other-hostname] \

[node-yet-another-hostname] \

--certs-dir=[path-to-certs-directory] \

--ca-key=[path-to-ca-key]

*# Create a client certificate and key:*

cockroach cert create-client \

[username] \

--certs-dir=[path-to-certs-directory] \

--ca-key=[path-to-ca-key]

*# List certificates and keys:*

cockroach cert list \

--certs-dir=[path-to-certs-directory]

*# View help:*

cockroach cert --help

cockroach cert create-ca --help

cockroach cert create-node --help

cockroach cert create-client --help

cockroach cert list --help

Flags

客户端连接

| **Flag** | **简介** |
| --- | --- |
| --certs-dir | 证书目录的路径  **Default:** ${HOME}/.cockroach-certs/ |
| --ca-key | CA密钥的路径，在执行create-\*子命令的时候需要使用该Flag。  **Env Variable:** COCKROACH\_CA\_KEY |
| --allow-ca-key-reuse | 代表执行create-ca子命令创建CA证书时允许复用--ca-key指定的目录当中已有的CA密钥文件，默认情况下CA密钥文件将重新生成。 |
| --overwrite | 代表执行create-\*子命令时证书密钥文件允许被覆写。 |
| --lifetime | 证书剩余的有效时间，格式内容为时分秒。  **Default:** 87840h0m0s (10 years) |
| --key-size | CA、节点、客户端验证对应的密钥的大小，单位为bit。  **Default:** 2048 |

日志

cockroach cert默认输出日志错误到stderr，更丰富的日志功能可查看：[日志行为](https://www.cockroachlabs.com/docs/stable/debug-and-error-logs.html)

示例

创建CA证书和密钥文件

创建归档目录

* certs用于存放生成的CA证书和所有节点和客户端的证书和密钥文件，其中部分的文件会传输到节点机器上。
* my-safe-directory用于存放生成的CA密钥文件，在之后为节点和用户创建证书和密钥的时候使用。

mkdir certs

mkdir my-safe-directory

创建CA证书和密钥文件

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

ls -l certs

total 8

-rw-r--r-- 1 maxroach maxroach 1.1K Jul 10 14:12 ca.crt

创建节点证书和密钥文件

对于每个节点进行如下操作：

cockroach cert create-node <nodeN>.example.com <nodeN>.another-example.com --certs-dir=certs --ca-key=my-safe-directory/ca.key

将证书和密钥传输到对应节点

*# Create the certs directory:*

ssh <username>@<**node** address> "mkdir certs"

*# Upload the CA certificate and node certificate and key:*

scp certs/ca.crt certs/**node**.crt certs/**node**.key \

<username>@<**node** address>:~/certs

删除本地机器的证书和密钥缓存

rm certs/node.crt certs/node.key

**TIPS:** 考虑为所有节点生成的证书和密钥文件都是同样的文件名，删除证书和密钥文件是有必要的。在默认情况下，只有为cockroach cert create-node命令添加--overwrite标签才会覆盖已有的同名的证书和密钥文件。

创建客户端证书和密钥文件

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

ls -l certs

total 40

-rw-r--r-- 1 maxroach maxroach 1.1K Jul 10 14:12 ca.crt

-rw-r--r-- 1 maxroach maxroach 1.1K Jul 10 14:13 client.maxroach.crt

-rw------- 1 maxroach maxroach 1.6K Jul 10 14:13 client.maxroach.key

-rw-r--r-- 1 maxroach maxroach 1.2K Jul 10 14:17 node.crt

-rw------- 1 maxroach maxroach 1.6K Jul 10 14:17 node.key

列举所有证书与密钥文件

cockroach cert list --certs-dir=certs

Certificate directory: certs

+-----------------------+---------------------+---------------------+------------+--------------------------------------------------------+-------+

| Usage | Certificate File | Key File | Expires | Notes | Error |

+-----------------------+---------------------+---------------------+------------+--------------------------------------------------------+-------+

| Certificate Authority | ca.crt | | 2027/07/18 | num certs: 1 | |

| Node | node.crt | node.key | 2022/07/14 | addresses: node2.example.com,node2.another-example.com | |

| Client | client.maxroach.crt | client.maxroach.key | 2022/07/14 | user: maxroach | |

+-----------------------+---------------------+---------------------+------------+--------------------------------------------------------+-------+

(3 rows)