使用 TLS（Transport Layer Security）保护通信

Fabric 支持节点之间使用 TLS 进行安全通信。TLS 通信可以使用单向（仅服务器）和双向（服务器和客户端）身份验证。

为 Peer 节点配置 TLS

Peer 节点既是 TLS 服务器又是 TLS 客户端。当另一个 Peer 节点、应用程序或客户端与其建立连接时，它是前者；而当它与另一个 Peer 节点或排序节点建立连接时，则是后者。

要在 Peer 节点上启用 TLS，需要设置以下配置：

- `peer.tls.enabled` = `true`
- `peer.tls.cert.file` = 包含 TLS 服务器证书文件的标准路径
- `peer.tls.key.file` = 包含 TLS 服务器私钥文件的标准路径
- `peer.tls.rootcert.file` = 包含颁发 TLS 服务器证书 CA 证书链的标准路径

默认情况下，在 Peer 节点上启用 TLS 时，TLS 客户端身份验证是关闭的。这意味着在 TLS 握手期间，Peer 节点将不会验证客户端（另一个 Peer 节点、应用程序或CLI）的证书。要在 Peer 节点上启用TLS 客户端身份验证，需要将节点配置中的属性 `peer.tls.clientAuthRequired` 设置为 `true` ，并将 `peer.tls.clientRootCAs.files` 属性设置为为客户端发布 TLS 证书 CA 证书链文件。

默认情况下，Peer 节点在充当 TLS 服务器和客户端时将使用相同的证书和私钥对。要在客户端使用其他证书和私钥对，请将 `peer.tls.clientCert.file` 和 `peer.tls.clientKey.file` 配置属性分别设置为客户端证书和密钥文件的标准路径。

也可以通过设置以下环境变量来启用具有客户端身份验证的 TLS：

- `CORE_PEER_TLS_ENABLED` = `true`
- `CORE_PEER_TLS_CERT_FILE` = 服务器证书的标准路径
- `CORE_PEER_TLS_KEY_FILE` = 服务器私钥的标准路径
- `CORE_PEER_TLS_ROOTCERT_FILE` = CA 证书链文件的标准路径
- `CORE_PEER_TLS_CLIENTAUTHREQUIRED` = `true`
- `CORE_PEER_TLS_CLIENTROOTCAS_FILES` = CA 证书链文件的标准路径
- `CORE_PEER_TLS_CLIENTCERT_FILE` = 客户证书的标准路径
- `CORE_PEER_TLS_CLIENTKEY_FILE` = 客户端密钥的标准路径

在 Peer 节点上启用客户端身份验证后，要求客户端在 TLS 握手期间发送其证书。如果客户端未发送其证书，则握手将失败，并且 Peer 节点将关闭连接。

当 Peer 节点加入通道时，将从通道的配置区块中读取通道成员的根 CA 的证书链，并将其添加到 TLS 客户端和服务端根 CA 的数据结构中。之后， Peer 节点间通信和 Peer 节点与排序节点间通信将会无缝地工作。

为排序节点配置 TLS

要在排序节点上启用 TLS，需要设置排序节点的配置:

- `General.TLS.Enabled` = `true`
- `General.TLS.PrivateKey` = 包含服务器私钥的文件的标准路径
- `General.TLS.Certificate` = 包含服务器证书的文件的标准路径
- `General.TLS.RootCAs` = 包含颁发 TLS 服务器证书 CA 证书链的标准路径

默认情况下，与 Peer 节点一样，排序节点上的 TLS 客户端身份验证处于关闭状态。要启用 TLS 客户端身份验证，需要设置以下配置属性：

- `General.TLS.ClientAuthRequired` = `true`
- `General.TLS.ClientRootCAs` = 包含颁发 TLS 服务器证书 CA 证书链的标准路径

也可以通过设置以下环境变量来启用具有客户端身份验证的 TLS ：

- `ORDERER_GENERAL_TLS_ENABLED` = `true`
- `ORDERER_GENERAL_TLS_PRIVATEKEY` = 包含服务器私钥的文件的标准路径
- `ORDERER_GENERAL_TLS_CERTIFICATE` = 包含服务器证书的文件的标准路径
- `ORDERER_GENERAL_TLS_ROOTCAS` = 包含颁发 TLS 服务器证书 CA 证书链的标准路径
- `ORDERER_GENERAL_TLS_CLIENTAUTHREQUIRED` = `true`
- `ORDERER_GENERAL_TLS_CLIENTROOTCAS` = 包含颁发 TLS 服务器证书 CA 证书链的标准路径

为节点 CLI 配置 TLS

针对启用了 TLS 的 Peer 节点运行 CLI 命令时，必须设置以下环境变量：

- `CORE_PEER_TLS_ENABLED` = `true`
- `CORE_PEER_TLS_ROOTCERT_FILE` = 包含颁发 TLS 服务器证书 CA 证书链的标准路径

如果在远程服务器上也启用了 TLS 客户端身份验证，则除上述变量外，还必须设置以下变量：

- `CORE_PEER_TLS_CLIENTAUTHREQUIRED` = `true`
- `CORE_PEER_TLS_CLIENTCERT_FILE` = 客户端证书的标准路径
- `CORE_PEER_TLS_CLIENTKEY_FILE` = 客户端私钥的标准路径

当运行连接到排序服务的命令时，例如 *peer channel <create|update|fetch>* 或 *peer chaincode <invoke>*，如果在排序节点上启用了 TLS ，则还必须指定以下命令行参数：

- –tls
- –cafile <包含排序节点 CA 证书链的文件的标准路径>

如果在排序节点上启用了 TLS 客户端身份验证，则还必须指定以下参数：

- –clientauth
- –keyfile <包含客户端私钥的文件的标准路径>
- –certfile <包含客户端证书的文件的标准路径>

调试 TLS 问题

在调试 TLS 问题之前，建议同时在 TLS 客户端和服务器端启用 `GRPC debug` 以获取附加信息。要启用 `GRPC debug`，需要在环境变量 `FABRIC_LOGGING_SPEC` 中加入 `grpc=debug` 。例如，如要将默认日志记录级别设置为 `INFO`，将 GRPC 日志记录级别设置为 `DEBUG`，则需先将日志记录规范设置为 `grpc=debug:info`。

如果您在客户端看到错误消息 `remote error: tls: bad certificate`，则通常表示 TLS 服务器已启用客户端身份验证，并且该服务器未收到正确的客户端证书，或者收到了不信任的客户端证书。请确保客户端正在发送其证书，并且该证书已被 Peer 节点或排序节点信任的 CA 证书所签名。

如果在链码日志中看到错误消息 `remote error: tls: bad certificate`，请确保链码是使用 Fabric v1.1 或更高版本的程序构建的。