

OpenLDAP启用TLS认证

朱超杰

Version 1.0.0, July 16, 2020

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision History** | | | |
| **Version** | **Author** | **Description** | **Date** |
| 1.0.0 | 朱超杰 | OpenLDAP启用TLS | 2020/07/16 |

# 文档编写目的

本文主要介绍在已部署的OpenLDAP基础上如何开启TLS认证。

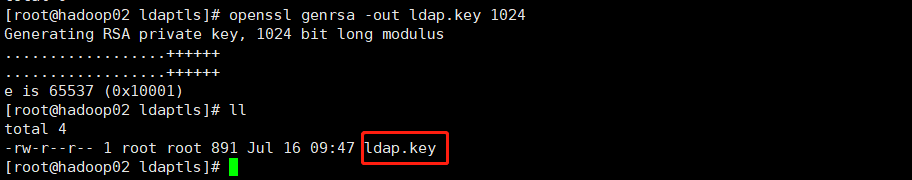
* 测试环境

1. OS版本为：Red Hat Enterprise 7.6
2. OpenLDAP版本为： 2.4.44
3. 操作用户：root

# TLS文件生成

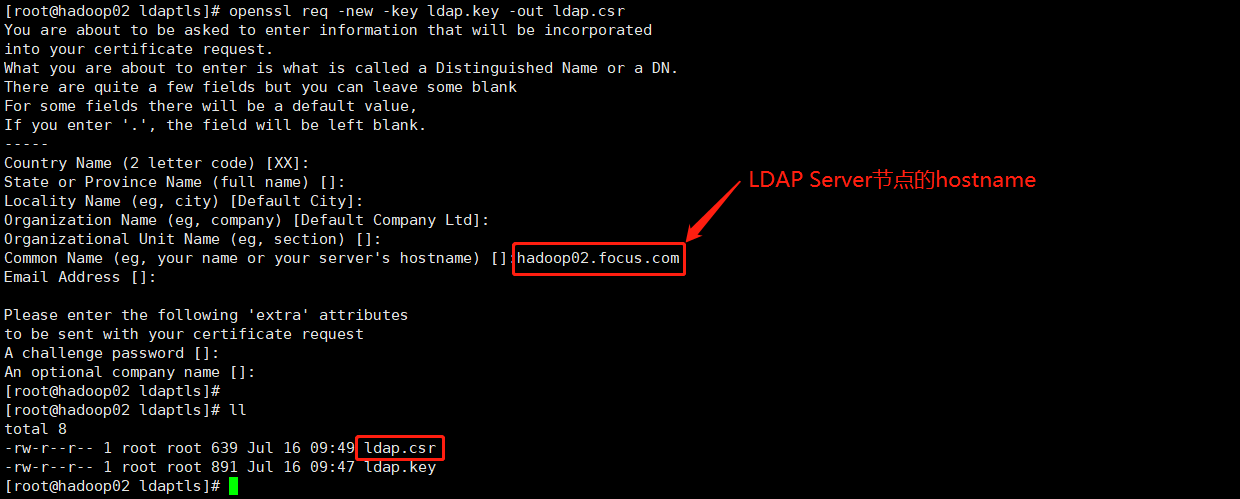
1. 生成RSA服务器私钥:

openssl genrsa -out ldap.key 1024



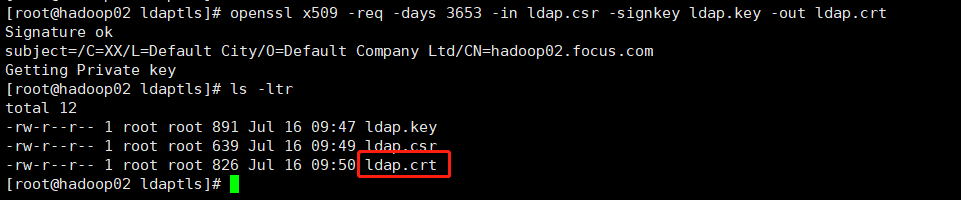
1. 生成签名文件:

openssl req -new -key ldap.key -out ldap.csr



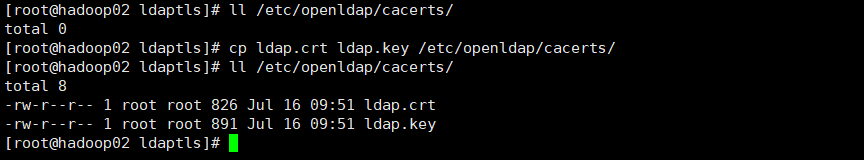
1. 生成公钥文件:

openssl x509 -req -days 3653 -in ldap.csr -signkey ldap.key -out ldap.crt



1. 将生成的公钥和私钥拷贝到/etc/openldap/cacerts/目录下:

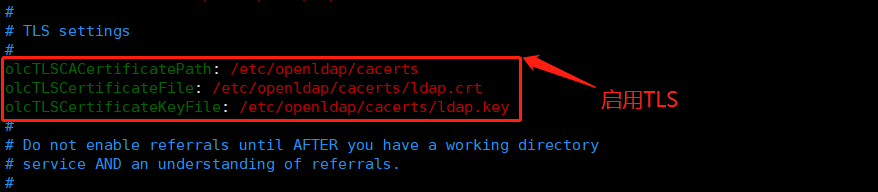
cp ldap.crt ldap.key /etc/openldap/cacerts/



# LDAP配置修改

1. 修改slapd.ldif文件（默认位置：/usr/share/openldap-servers），添加TLS配置

vim /usr/share/openldap-servers/slapd.ldif

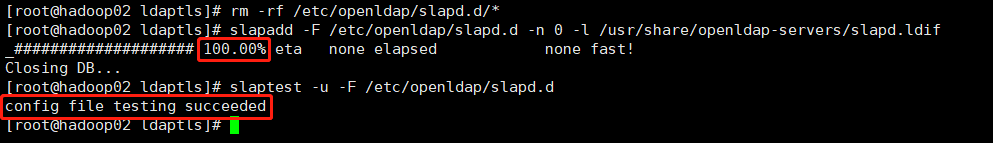


1. 如下命令重新生成OpenLDAP配置文件，并测试配置文件是否正确：

rm -rf /etc/openldap/slapd.d/\*

slapadd -F /etc/openldap/slapd.d -n 0 -l /usr/share/openldap-servers/slapd.ldif

slaptest -u -F /etc/openldap/slapd.d



执行如下命令修改配置文件的属主，然后重启slapd服务

chown -R ldap. /etc/openldap/slapd.d/

ll /etc/openldap/slapd.d/

systemctl restart slapd

systemctl status slapd

