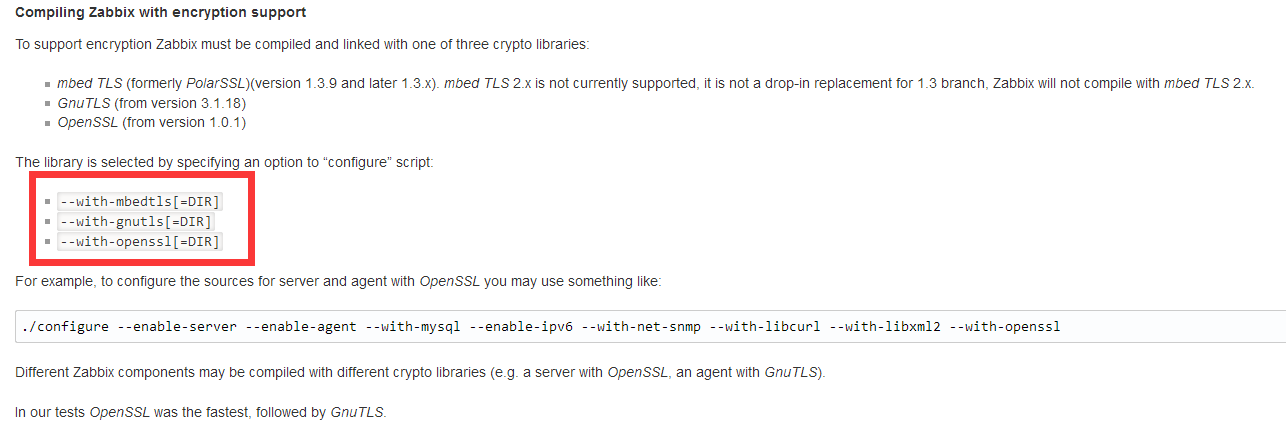
Zabbix 配置数字证书加密 邹立翔 2017年4月27日

官方文档

但默认情况下，zabbix是通过不安全的线路进行传输的，有可能造成数据泄露等危险，为此我为我的zabbix服务添加数据证书的配置以便通过加密通道传输数据。

https://www.zabbix.com/documentation/3.0/manual/encryption

一，配置zabbix依赖包和扩展包（因为我的zabbix是后期加的数字加密，所以的扩展）





下载以后两个包

1. 安装mbedtls-mbedtls

https://codeload.github.com/ARMmbed/mbedtls/tar.gz/mbedtls-1.3.19

1. tar xf mbedtls-mbedtls-1.3.19.tar.gz
2. cd mbedtls-mbedtls-1.3.19
3. make SHARED=1 CFLAGS=-fPIC
4. make DESTDIR=/usr install
5. Ldconfig

下载gnutls

ftp://mirror.switch.ch/pool/4/mirror/fedora/linux/releases/25/Workstation/source/tree/Packages/g/gnutls-3.5.5-2.fc25.src.rpm

1. rpm -ivh gnutls-3.5.5-2.fc25.src.rpm

安装完之后重新编译之前的zabbix server

cd zabbix-3.0.4/

./configure --prefix=/usr/local/zabbix --sysconfdir=/etc/zabbix/ --enable-server --enable-proxy --enable-agent --with-mysql=/usr/local/mysql/bin/mysql\_config --with-net-snmp --with-libcurl --with-libxml2 --with-openssl

make

make install

在重启zabbix server

zabbix\_server -c /etc/zabbix/zabbix\_server.conf

zabbix\_agentd -c /etc/zabbix/zabbix\_agentd.conf

二 ，配置数字证书

当配置好zabbix服务端和agent后，即可继续配置数字证书的部分，首先需要使用openssl生成数字证书。

我们需要先生成ca证书，然后通过ca证书签发服务器证书与客户端证书。先建立一个文件夹以便存放所有证书文件：

#新建文件夹

mkdir zabbix\_crt

#进入文件夹

cd zabbix\_crt

然后使用以下命令建立所需要的证书文件。其中CN部分可以修改为服务器的域名或IP，在实际应用中推荐修改为服务器的域名：

openssl genrsa 2048 > ca.key

cat ca.key

openssl req -new -x509 -nodes -days 1000 -key ca.key -subj /CN=Signing\ CA/OU=Development\ group/O=Zabbix\ SIA/DC=zabbix/DC=com > ca.crt

openssl req -newkey rsa:2048 -days 1000 -nodes -keyout server.key -subj /CN=server/OU=Development\ group/O=Zabbix\ SIA/DC=zabbix/DC=com > server.csr

openssl x509 -req -in server.csr -days 1000 -CA ca.crt -CAkey ca.key -set\_serial 01 > server.crt

openssl req -newkey rsa:2048 -days 1000 -nodes -keyout client.key -subj /CN=client/OU=Development\ group/O=Zabbix\ SIA/DC=zabbix/DC=com > client.csr

openssl x509 -req -in client.csr -days 1000 -CA ca.crt -CAkey ca.key -set\_serial 01 > client.crt

cp ca.crt /etc/zabbix/zabbix\_crt/

cp server.crt /etc/zabbix/zabbix\_crt/

cp server.key /etc/zabbix/zabbix\_crt/

Zabbix\_crt下面的文件添加权限

chown zabbix:zabbix ca.crt server.\*

三，修改zabbix服务端 的配置文件

vi /etc/zabbix/zabbix\_server.conf

#修改TLSCAFile配置

TLSCAFile=/usr/local/zabbix/zabbix\_crt/ca.crt

#修改TLSCertFile配置

TLSCertFile=/usr/local/zabbix/zabbix\_crt/server.crt

#修改TLSKeyFile配置

TLSKeyFile=/usr/local/zabbix/zabbix\_crt/server.key

在重启zabbix server

zabbix\_server -c /etc/zabbix/zabbix\_server.conf

zabbix\_agentd -c /etc/zabbix/zabbix\_agentd.conf

客户端

客户端和服务端类似，现在agent目录建立一个文件夹，然后将以下文件复制到该文件夹中：

* ca.crt
* client.crt
* client.key

scp -P 60158 ca.crt root@192.168.2.141:/etc/zabbix/zabbix\_crt

scp -P 60158 client.crt client.key root@192.168.2.141:/etc/zabbix/zabbix\_crt

配置客户端的文件

cd /etc/zabbix/

vi zabbix\_agentd.conf

TLSConnect=cert

TLSAccept=cert

TLSCAFile=/etc/zabbix/zabbix\_crt/ca.crt

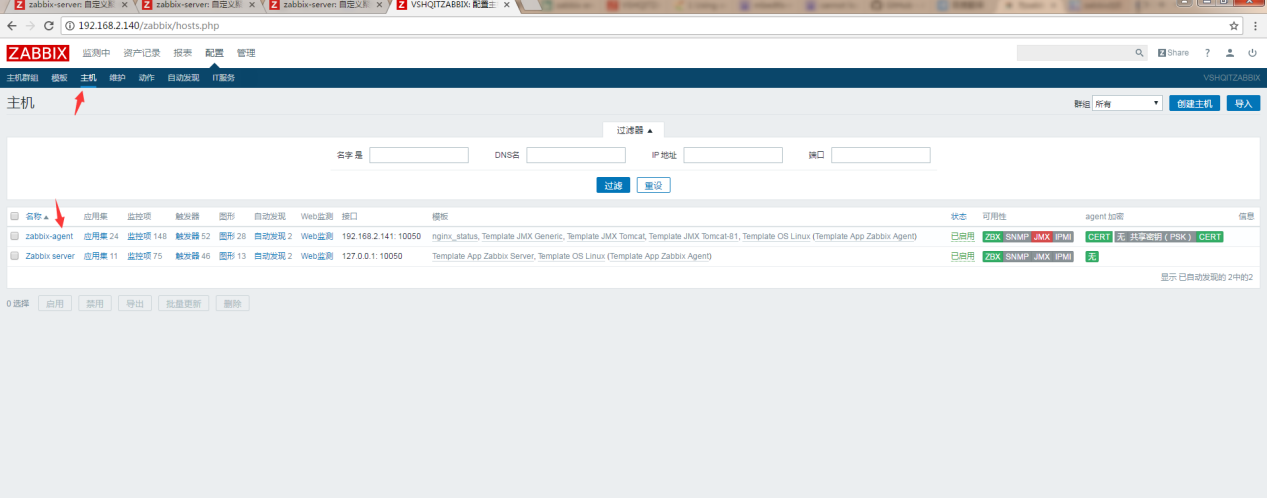
TLSCertFile=/etc/zabbix/zabbix\_crt/client.crt

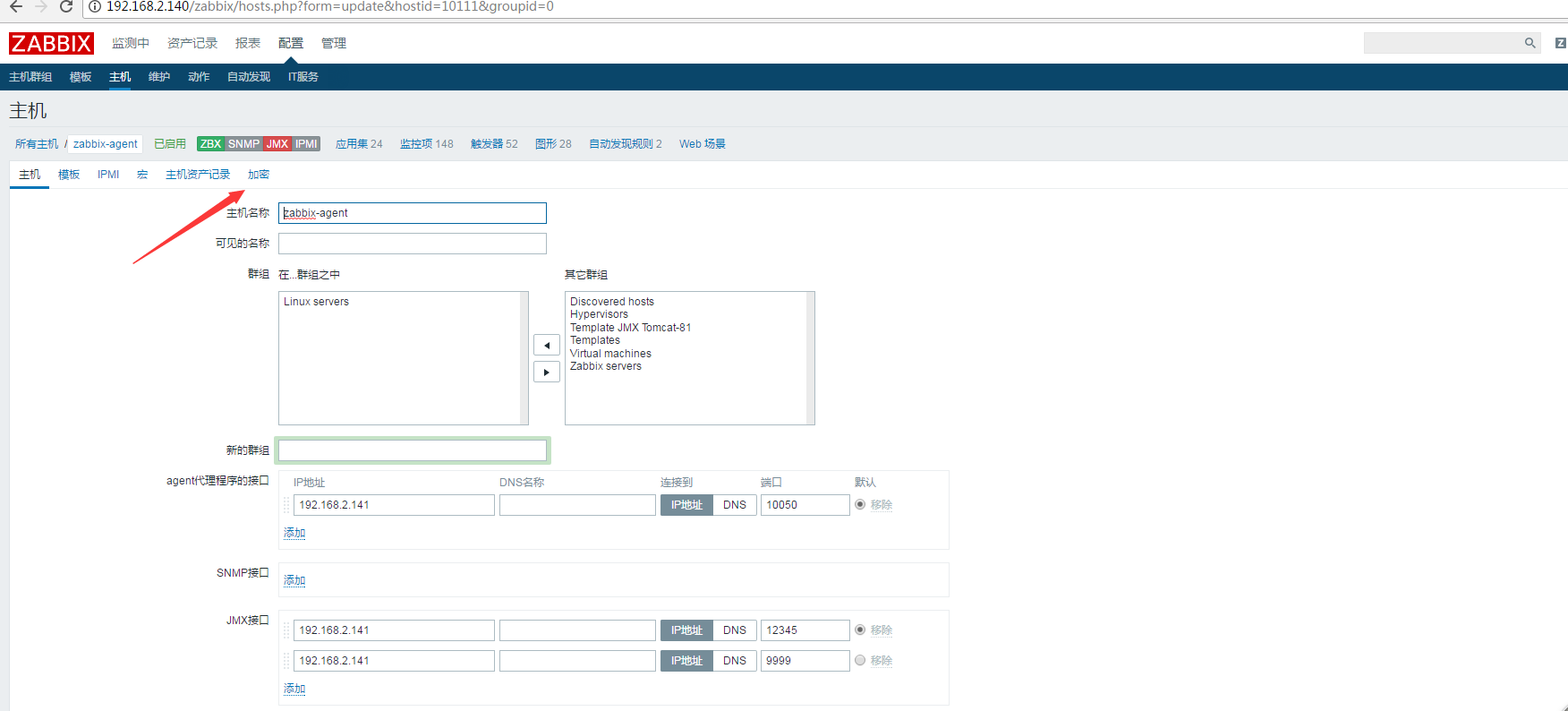
TLSKeyFile=/etc/zabbix/zabbix\_crt/client.key

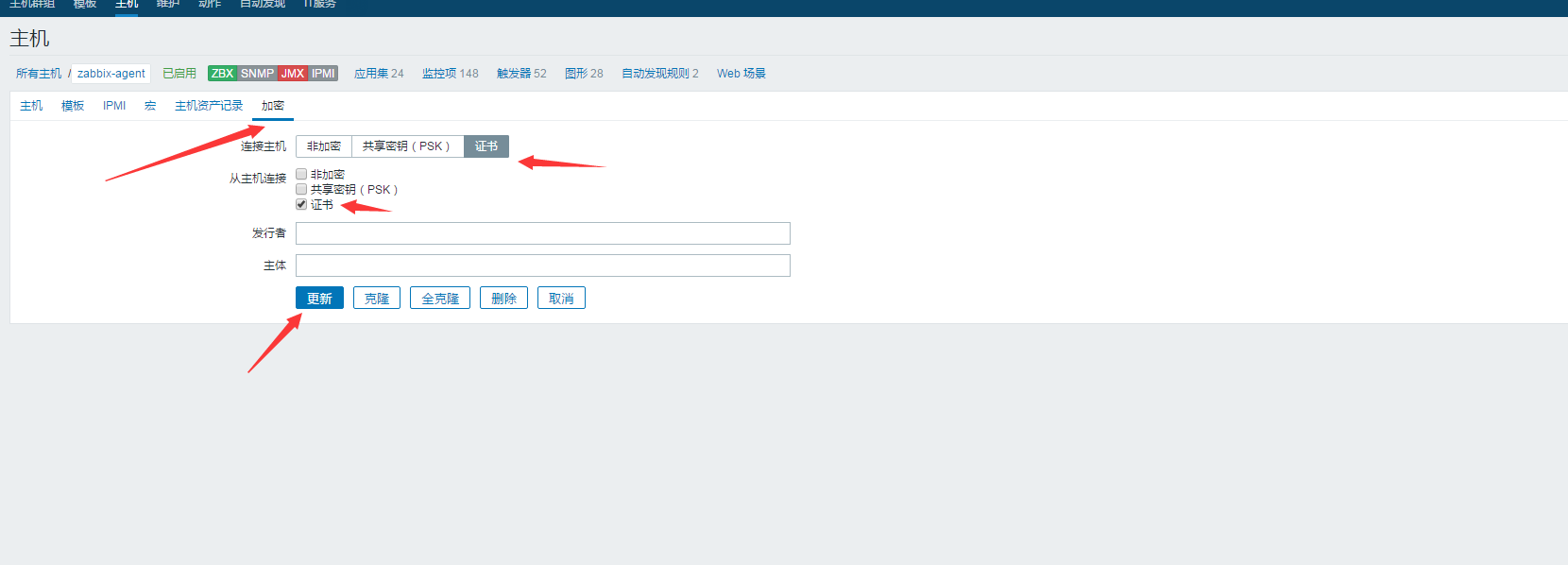
重启zabbix-agent

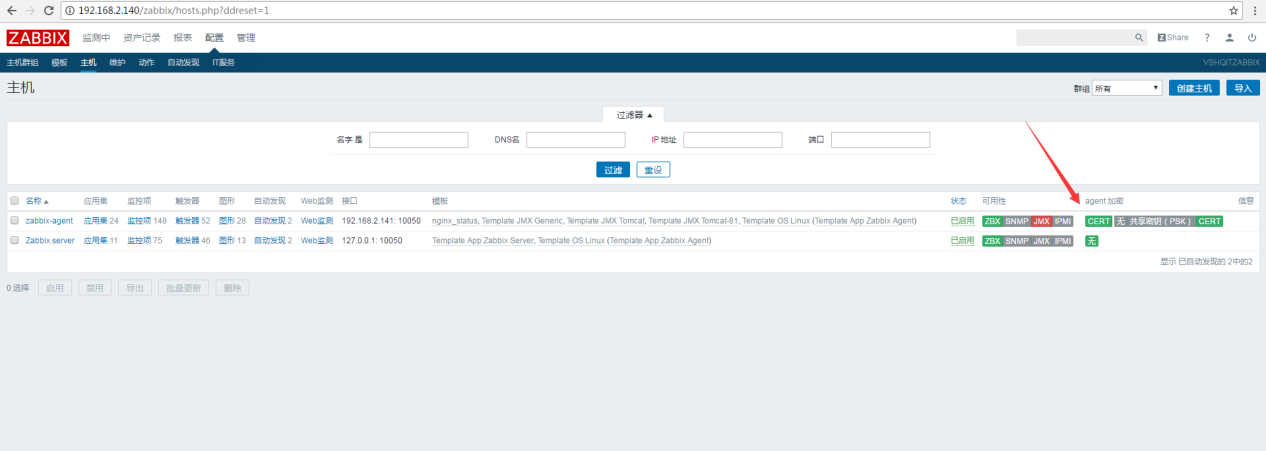
/etc/init.d/zabbix-agent restart

Web界面添加证书









最后看到绿色就成功了

如果对安全性有更高要求，还可以使用商业数字证书或免费的数字证书（例如：[为strongswan配置Encryption Everywhere项目的证书](https://enginx.cn/2016/12/12/%e4%b8%bastrongswan%e9%85%8d%e7%bd%aeencryption-everywhere%e9%a1%b9%e7%9b%ae%e7%9a%84%e8%af%81%e4%b9%a6.html" \t "https://enginx.cn/2017/01/08/_blank)）替换掉自签发的数字证书。