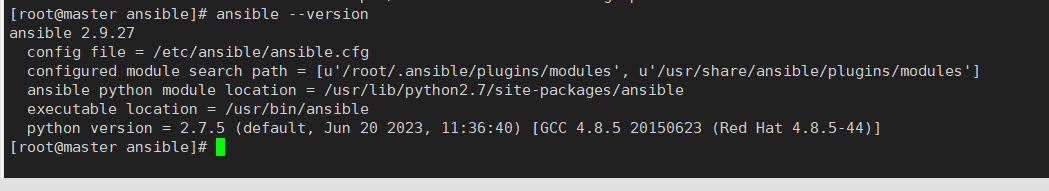
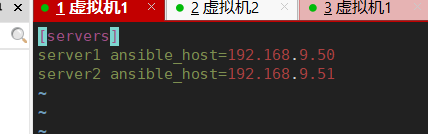
**使用ansible完成两台机器部署tomcat**

安装ansible，首先安装EPEL存储库： Ansible可以通过EPEL存储库进行安装

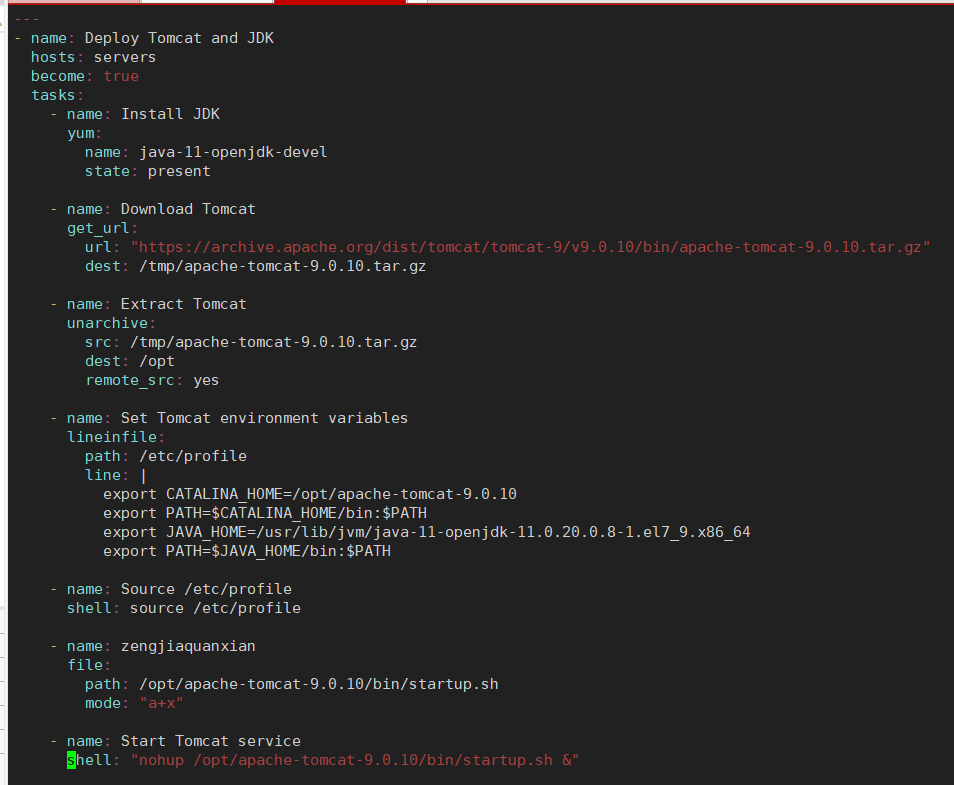
Yum install epel-release,执行完毕后执行yum install ansible,完成后验证



1. 创建 Ansible Inventory 文件，touch inventory.ini,写入如下内容



1. 创建 Ansible Playbook 文件，在Ansible 项目目录中创建一个名为 deploy\_tomcat.yml文件，写入如下内容

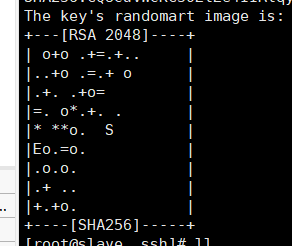


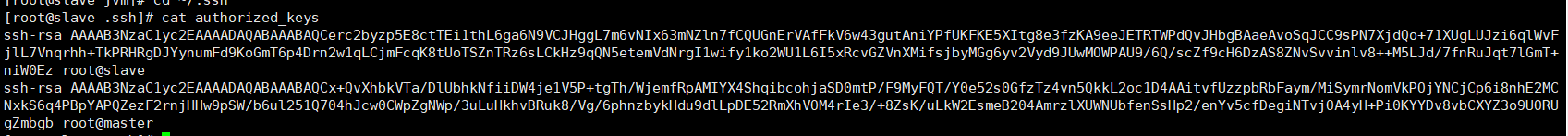
1. 输入cd ~/.ssh进入ssh目录，输入ssh-keygen生成密钥，复制公开密钥到两台机器的authorized\_keys文件下，用于身份验证，如下图所示

scp文件名 root@目标主机ip:/root/.ssh

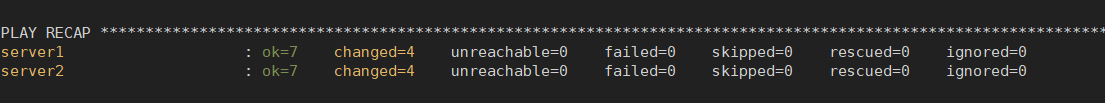
cp 目标主机公钥文件 authorized\_keys

cat 服务端公钥文件 >> authorized\_keys



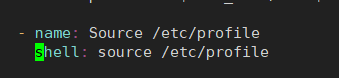


1. 在ansible目录下执行ansible-playbook -i inventory.ini deploy\_tomcat.yml，执行完毕如下图所示



**错误：**

1. 访问出错，访问被拒绝，生成ssh密钥，并分发到另一台机器解决
2. 环境变量写入路径出错，/etc/profile/修改为/etc/profile解决
3. playbook中写入source命令使文件profile生效时报错，这是因为Ansible的command模块无法直接执行source命令将命令写入shell解决，如下图所示



1. 在playbook中写入了启动tomcat模块，执行后命令不生效

- name: Start Tomcat service

shell: /opt/apache-tomcat-10.1.15/bin/startup.sh

执行完毕后未报错，发现tomcat未正常启动

- name: Start Tomcat service

command: /opt/apache-tomcat-10.1.15/bin/startup.sh

执行完毕后未报错，发现tomcat未正常启动

- name: Start Tomcat service

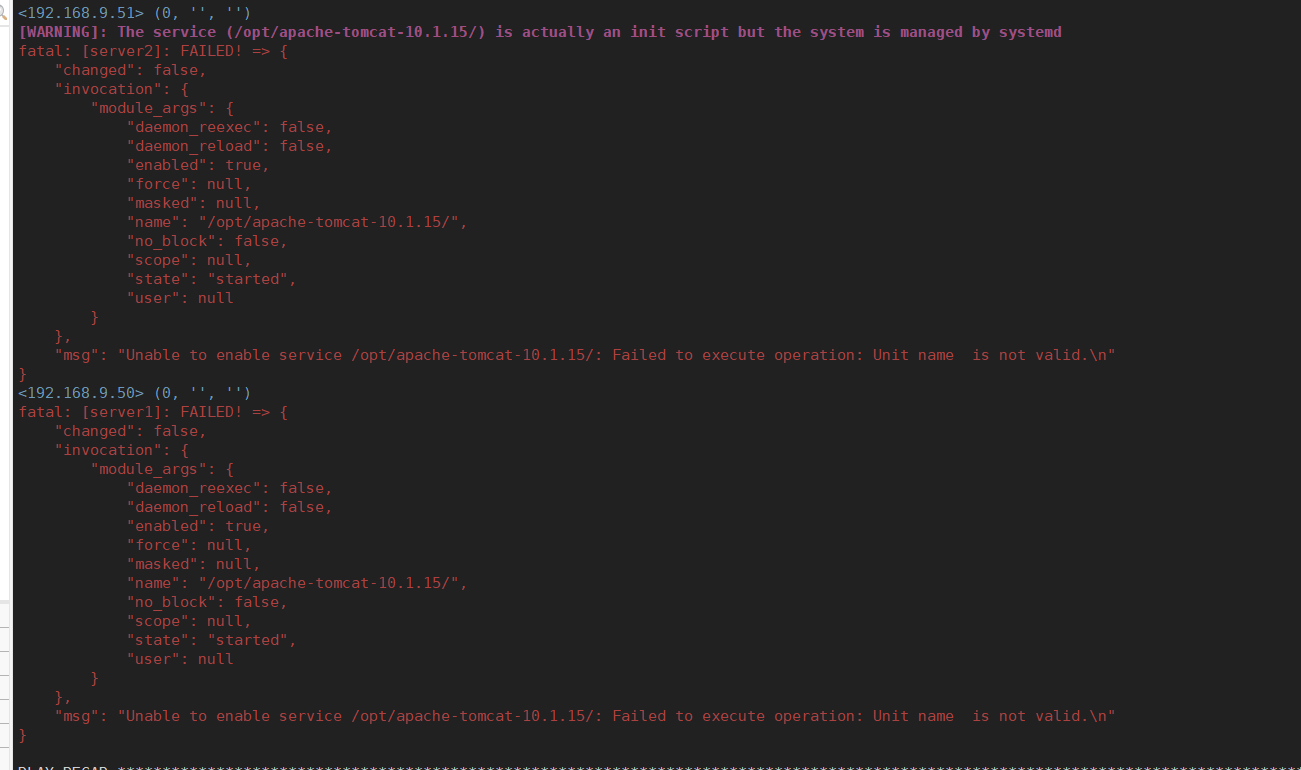
systemd:

name: tomcat

state: started

enabled: yes

执行完毕后报错



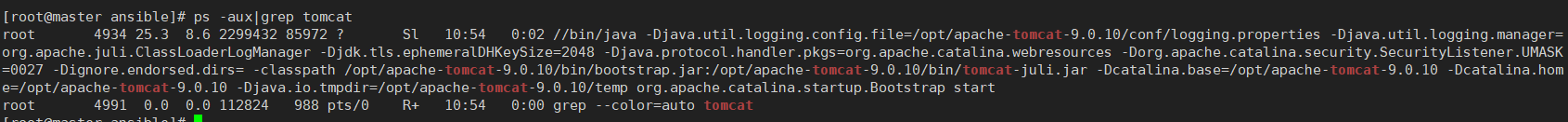
经百度得知，Tomcat安装是使用传统的init脚本而不是systemd单元文件，因此不能systemd模块来管理tomcat服务，应该用command模块或者shell，经试验command模块和shell也未能成功启动tomcat。

当涉及到管理和启动系统服务时，Linux系统使用两种不同的方法：传统的init脚本和现代的systemd单元文件。

传统的init脚本，每个服务都有一个对应的启动脚本，通常位于/etc/init.d/目录下，使用特定的命令如start、stop、restart来管理服务的状态。

Systemd单元文件，systemd使用单元文件（unit files）来描述和管理服务，通常位于/etc/systemd/system/目录下，可以使用systemctl命令来管理服务，这些单元文件通常位于/etc/systemd/system/目录或/usr/lib/systemd/system/目录下。

后更换tomcat版本，将tomcat10版本更换为tomcat9版本，问题解决，可以使用ansible启动tomcat

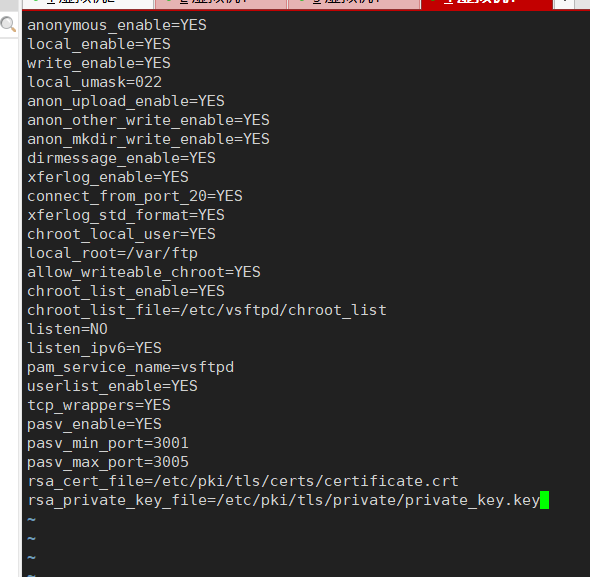


**安装vsftpd**

1. 创建vsftpd50.ini文件，写入如图内容



1. 创建vsftpd50.conf文件，用于写入vsftpd.conf配置文件，如下所示



anonymous\_enable=YES: 启用匿名用户登录。

local\_enable=YES: 启用本地用户登录。

write\_enable=YES: 允许用户进行写操作（上传、删除等）。

local\_umask=022: 设置本地用户创建文件和目录的默认权限掩码。

anon\_upload\_enable=YES: 允许匿名用户上传文件。

anon\_other\_write\_enable=YES: 允许匿名用户对已上传文件进行更改。

anon\_mkdir\_write\_enable=YES: 允许匿名用户创建目录。

dirmessage\_enable=YES: 启用目录显示消息。

xferlog\_enable=YES: 启用传输日志记录。

connect\_from\_port\_20=YES: 使用20端口进行数据连接。

xferlog\_std\_format=YES: 使用标准的xferlog格式记录日志。

chroot\_local\_user=YES: 将本地用户限制在其主目录中。

local\_root=/var/ftp: 设置本地用户的根目录路径。

allow\_writeable\_chroot=YES: 允许在chroot环境中写入。

chroot\_list\_enable=YES: 启用chroot用户列表。

chroot\_list\_file=/etc/vsftpd/chroot\_list: 指定包含允许chroot的用户列表的文件路径。

listen=NO: 禁用IPv4监听。

listen\_ipv6=YES: 启用IPv6监听。

pam\_service\_name=vsftpd: 指定用于PAM认证的服务名称。

userlist\_enable=YES: 启用用户列表。

tcp\_wrappers=YES: 启用TCP包装器，以控制对服务器的访问。

pasv\_enable=YES: 启用被动模式（Passive Mode）。

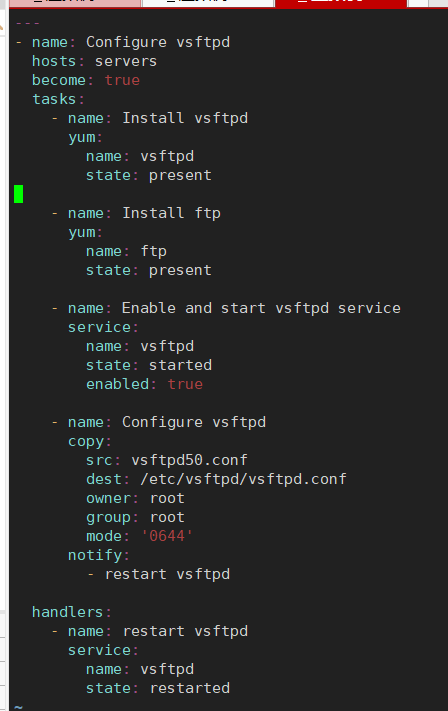
pasv\_min\_port=3001: 设置被动模式使用的最小端口。

pasv\_max\_port=3005: 设置被动模式使用的最大端口

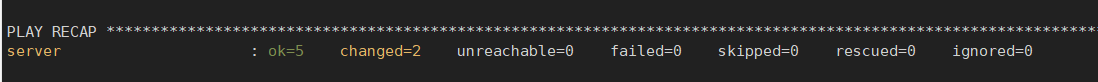
rsa\_cert\_file=/etc/pki/tls/certs/certificate.crt: 指定了用于TLS/SSL连接的服务器证书文件的路径。

rsa\_private\_key\_file=/etc/pki/tls/private/private\_key.key: 指定了用于TLS/SSL连接的服务器私钥文件的路径

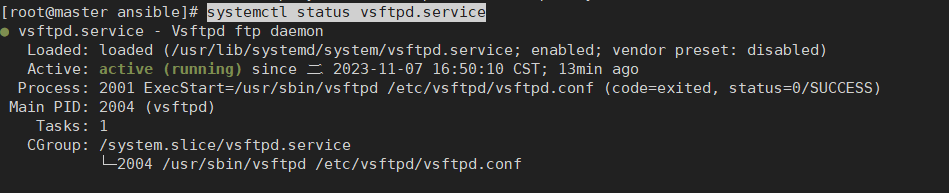
1. 创建Ansible Playbook文件vsftpd50.yml，写入如下内容



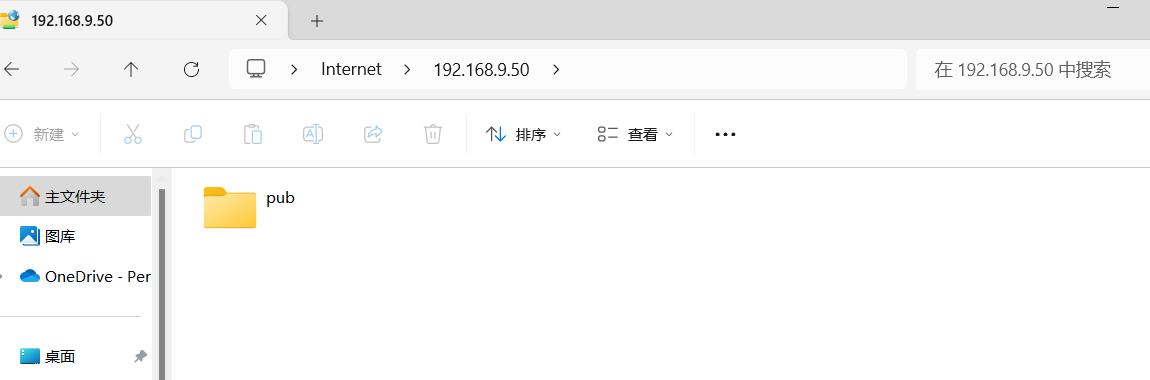
1. 输入ansible-playbook -i vsftpd50.ini vsftpd50.yml -vvv并执行，执行成功如图所示



1. 此时查看输入systemctl status vsftpd.service查看状态，如图所示

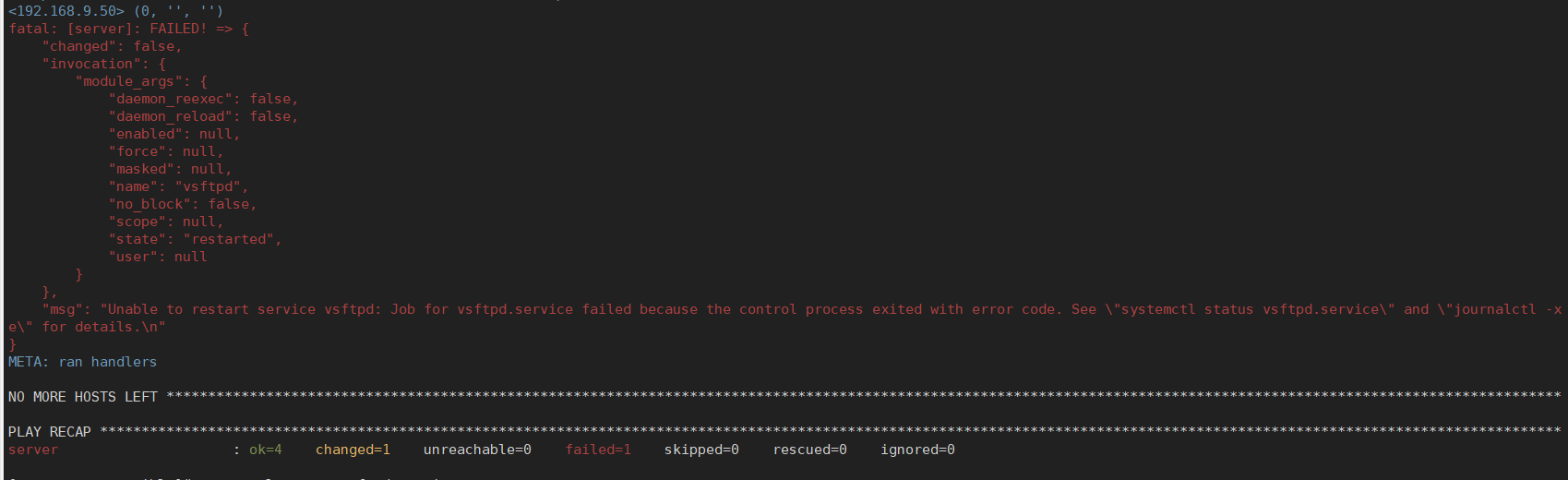


1. 输入ftp 192.168.9.50进行本地登录成功，配置另一台时，将vsftpd50.ini中的ip改为目标机器ip，并将vsftpd50.yml文件中pasv\_address=192.168.9.50ip改为目标机器ip，注意ssh密钥是否够成功配对

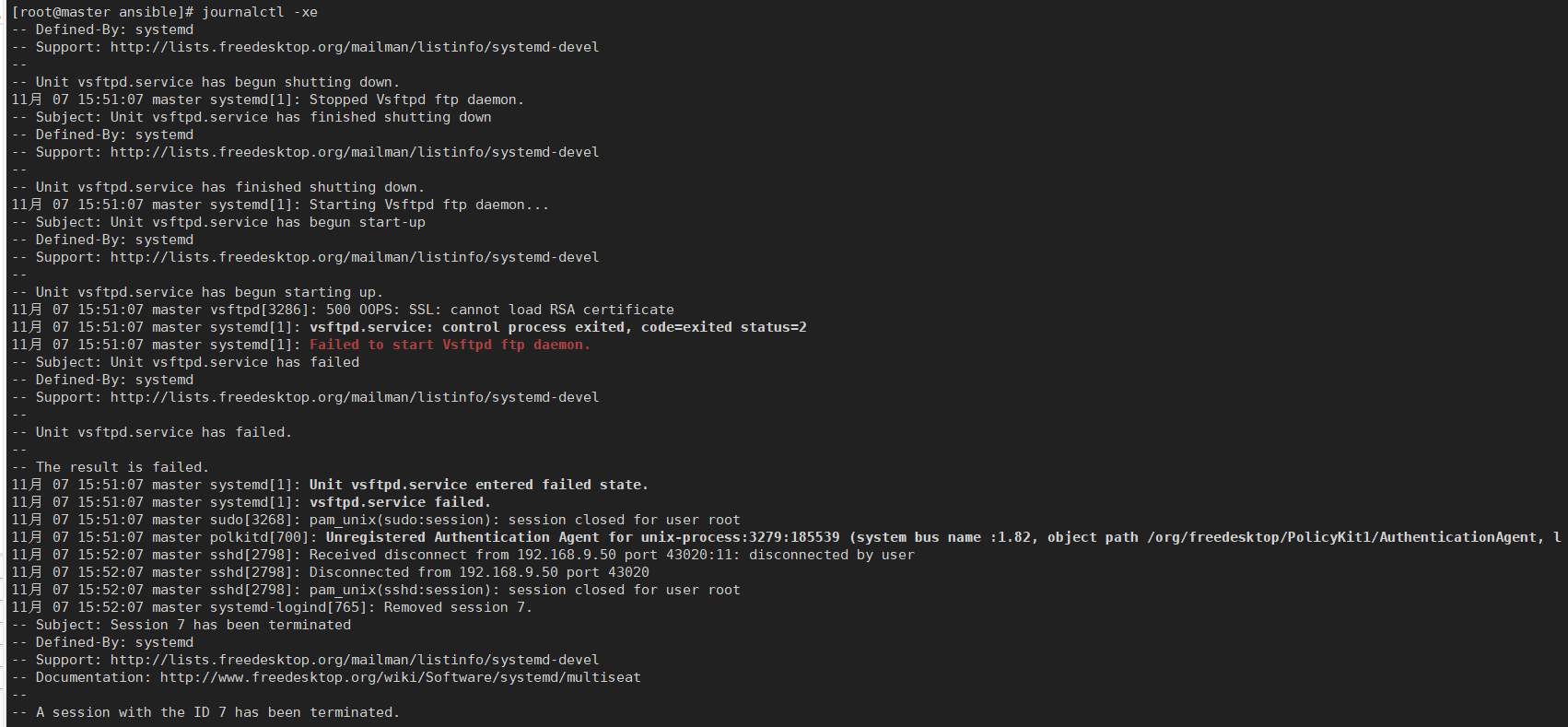


**错误：**

1. 执行ansible-playbook -i vsftpd50.ini vsftpd50.yml -vvv时，报如下错误



无法启动vsftpd服务，此时输入systemctl status vsftpd.service查看状态发现服务未启动，输入journalctl -xe获取详细信息



根据日志，vsftpd服务启动失败的原因是无法加载RSA证书，使用命令查看配置文件下的证书

openssl x509 -in /etc/pki/tls/certs/certificate.crt -text -noout

openssl rsa -in /etc/pki/tls/private/private\_key.key -check

查证，发现证书文件不存在，经百度，使用命令

openssl genpkey -algorithm RSA -out /etc/pki/tls/private/private\_key.key -pkeyopt rsa\_keygen\_bits:2048

生成一个2048位的RSA私钥文件，并将其保存在/etc/pki/tls/private/private\_key.key路径下openssl req -new -x509 -sha256 -key /etc/pki/tls/private/private\_key.key -out /etc/pki/tls/certs/certificate.crt -days 365

生成一个有效期为365天的自签名证书文件，并将其保存在/path/to/certificate.crt路径下

使用命令

chmod 600 /etc/pki/tls/private/private\_key.key

chmod 600 /etc/pki/tls/certs/certificate.crt

赋予证书文件为只有所有者可读写，问题解决。