**陕西省信息中心政务信息系统**

**基础架构使用指南**

**版本：1.0**

**应用技术处运维工作组**

**2020年3月**

目录

[1 VPN使用指南 2](#_Toc34824191)

[1.1 VPN设备遵循的国家标准 2](#_Toc34824192)

[1.2 VPN客户端支持的设备和操作系统 2](#_Toc34824193)

[1.3 VPN客户端的安装 2](#_Toc34824194)

[1.4 配置VPN客户端及注意事项 4](#_Toc34824195)

[2 虚拟机使用指南 14](#_Toc34824196)

[2.1 检查虚拟机配置 14](#_Toc34824197)

[2.2 查看和更改防火墙配置 16](#_Toc34824198)

[2.3 查看和更改磁盘配置 17](#_Toc34824199)

[2.4 检查和安装必要的组件 20](#_Toc34824200)

[2.5 与NTP服务器时间同步 21](#_Toc34824201)

[2.6 安装应用软件 26](#_Toc34824202)

[3 数据库使用指南 26](#_Toc34824203)

[3.1 ODA IP地址 26](#_Toc34824204)

[3.1.1 政务外网区ODA X6-2 IP地址 26](#_Toc34824205)

[3.1.2 政务外网区ODA X7-2 IP地址 26](#_Toc34824206)

[3.1.3 互联网区ODA X6-2 IP地址 26](#_Toc34824207)

[3.2 ODA中创建用户和表 27](#_Toc34824208)

[3.2.1 创建用户 27](#_Toc34824209)

[3.2.2 创建表 27](#_Toc34824210)

[4 附件1：运维工作组联系方式 29](#_Toc34824211)

# VPN使用指南

## VPN设备遵循的国家标准

省信息中心政务信息系统使用奥联研发的VPN智能网关。VPN智能网关采用NTLS传输协议和国密SM9、SM4算法实现安全虚拟专网组建，遵循国密标准GM/T 0022-2014《IPSec VPN 技术规范》和GM/T 0024-2014《SSL VPN技术规范》，支持国密IPSEC和国密SSL安全传输协议。

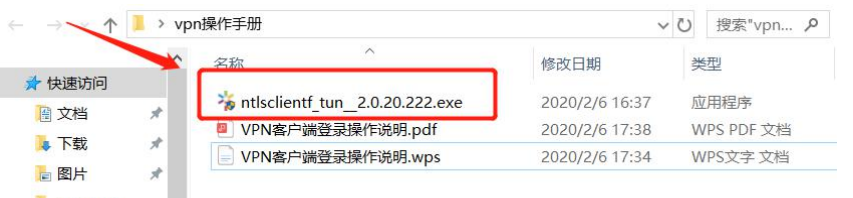
## VPN客户端支持的设备和操作系统

VPN客户端目前支持windows系统，其它操作系统暂不支持；

移动设备暂不支持。

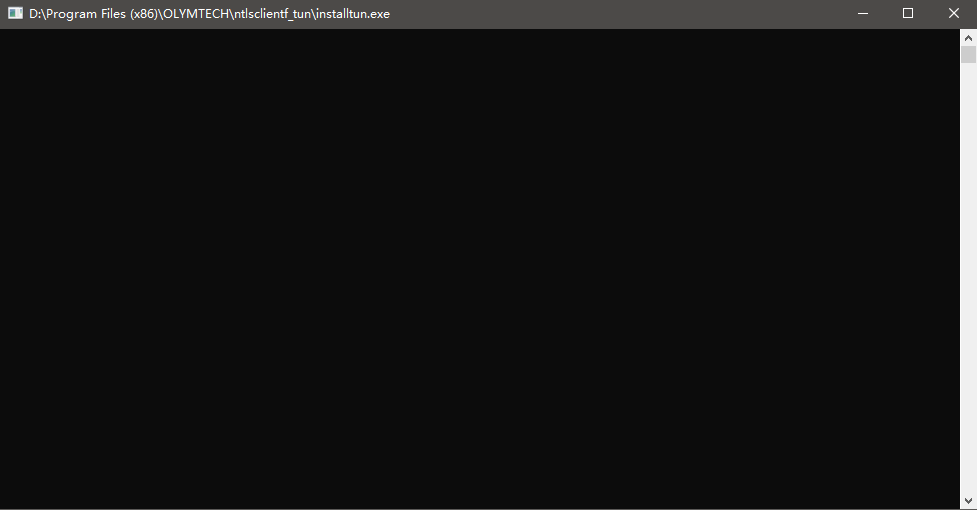
## VPN客户端的安装

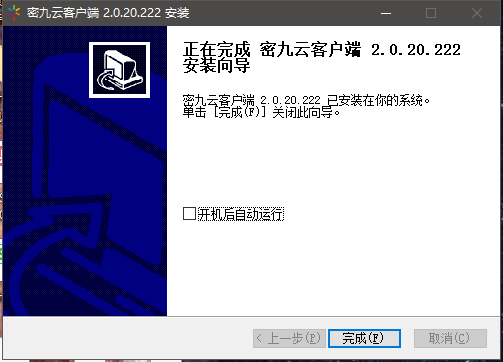
在文件夹中找到并执行“ntlsclientf\_tun\_\_2.0.20.222.exe”的文件。



根据安装导航进行下一步操作并完成安装。

弹出如下所示的黑色方框，请勿关闭。

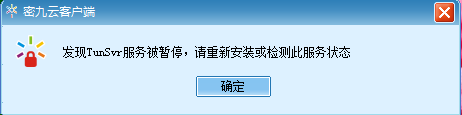




**注意事项：**

部分安全软件（如360安全卫士）会对VPN客户端的安装进行阻止。请点击右下角箭头标志选择“允许本次操作”，并勾选左下角“不再提醒”，若后续再次弹出类似阻止界面，请重复上述操作。

如未按照“**VPN安装说明及注意事项**”进行安装操作，打开VPN客户端时可能会出现以下提示，需要卸载VPN客户端并根据“**VPN安装说明及注意事项**”重新安装。



## 配置VPN客户端及注意事项

第一步，双击打开桌面所示VPN客户端图标。



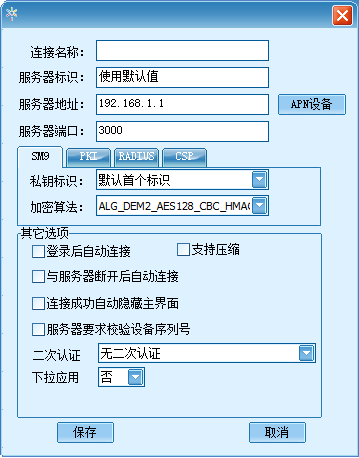
打开后会出现以下界面，请点击“确定”进行下一步操作。

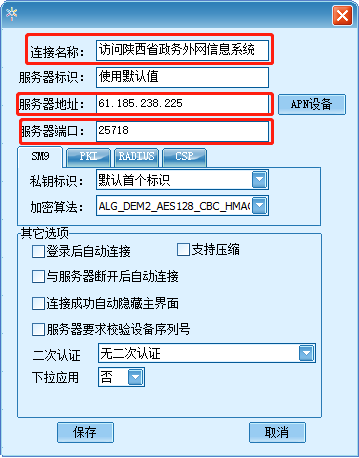


第二步，上述操作后会进入“连接管理”界面，点击“新建连接”。



点击“新建连接”后会进入如下图所示界面，此时我们对其进行编辑，**“连接名称”自行定义，“服务器地址”为“61.185.238.225”，“服务器端口”为“25718”，其他无需更改。**





编辑完成后，点击“保存”，并自动返回到“连接管理”界面。



完成上述操作后，请勿直接进行连接，需要进行密钥下载，否则会出现以下提示。

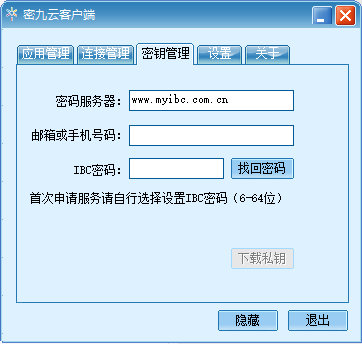


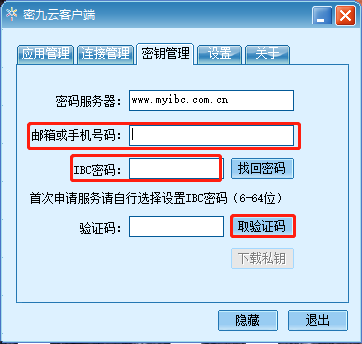
如出现上述界面请点击“确定”，并根据下述第三步步骤进行操作。

第三步，点击“密钥管理”，进行**“密钥下载”**。



点击后，会出现如下界面，**请在标记处输入您所注册的“手机号码”，并将您想设置的密码直接输入“IBC密码”一栏，输入完成后点击“获取验证码”**。





将获取到的验证码填入对应一栏中，并点击“下载私钥”。



第四步，下载私钥完成后点击“连接管理”，选择之前编辑的连接，并点击“连接”，并在弹出的界面输入您所设置的密码，输入完成后点击“确定”。





密码输入完成后，如下图所示，即代表连接成功。



连接成功后，即可访问己方所负责的应用及服务。

**注意事项：**

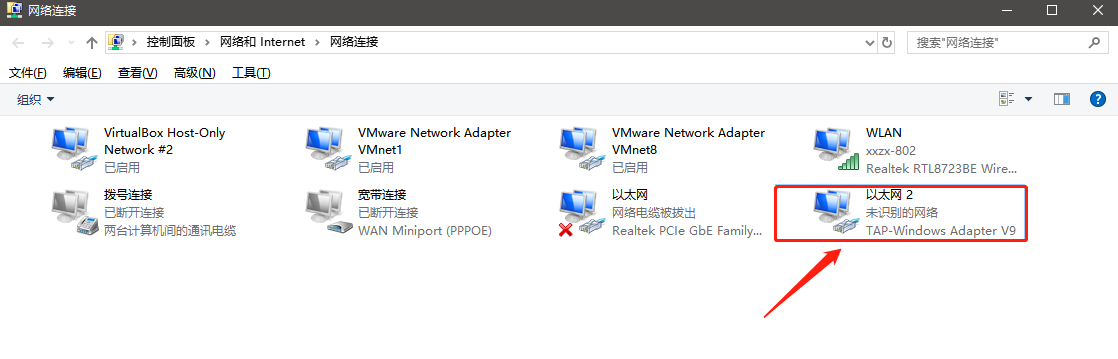
部分连接成功之后，无法正常访问可能有以下原因：

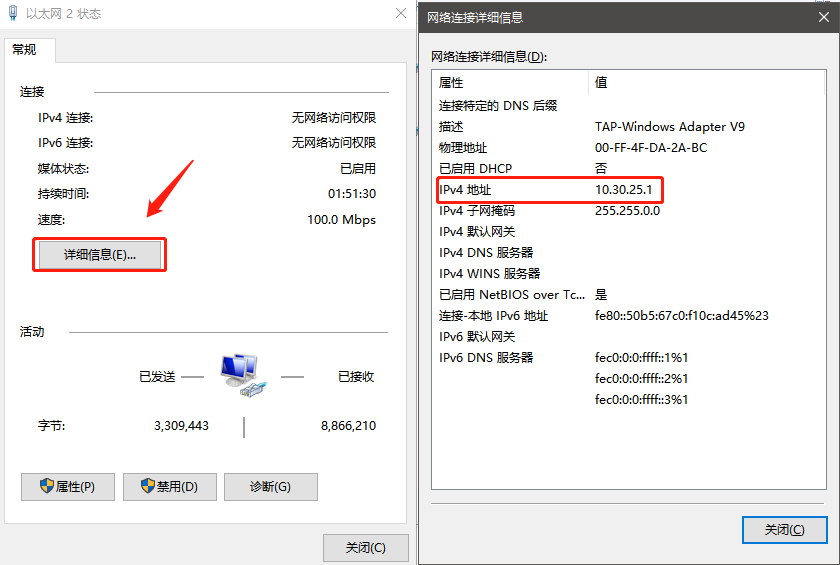
1.打开客户端时安全软件阻止，未点击“允许该操作”，提示如下图所示。此时将无法获取到正确的IP地址。



解决方法：将VPN客户端退出，并重新打开，弹出上图提示，点击“允许操作”，使VPN客户端获取到正确IP地址，IP地址范围为“10.30.25.1--10.30.30.254”，可在“控制面板--网络和internet--网络连接--以太网2--右键--状态--详细信息”中看到。如若不是，先将VPN退出，然后“控制面板--网络和internet--网络连接--以太网2--右键--禁用--右键--启用”，重新打开VPN，即可获取正确正确的IP地址。

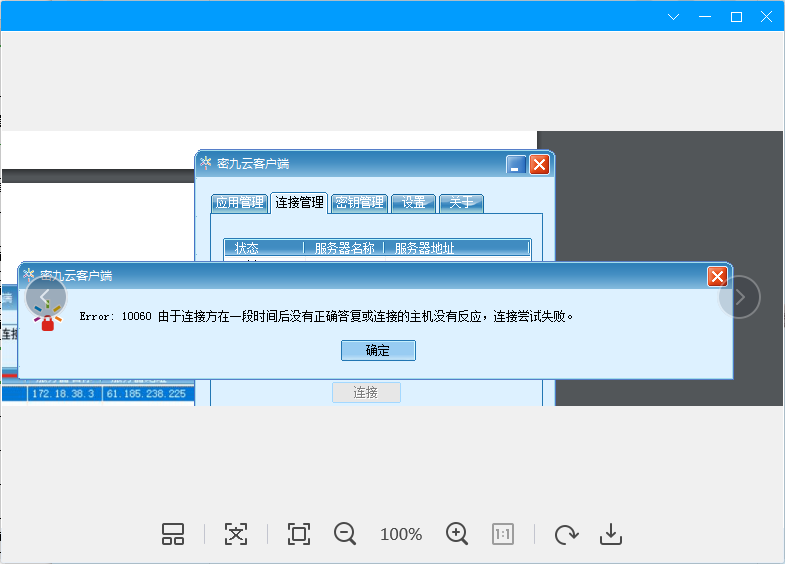


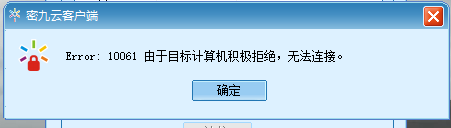




2.确认自己是否是已经注册的VPN账号，未注册的VPN账号无法获取正确的IP地址，故无法访问。

3.连接VPN出现下图所示问题时，原因所编辑的连接未按照文档所述编辑填写，请严格对照文档“VPN客户端使用说明”所列内容填写连接管理。完成之后重新连接，即可连接成功。





# 虚拟机使用指南

## 检查虚拟机配置

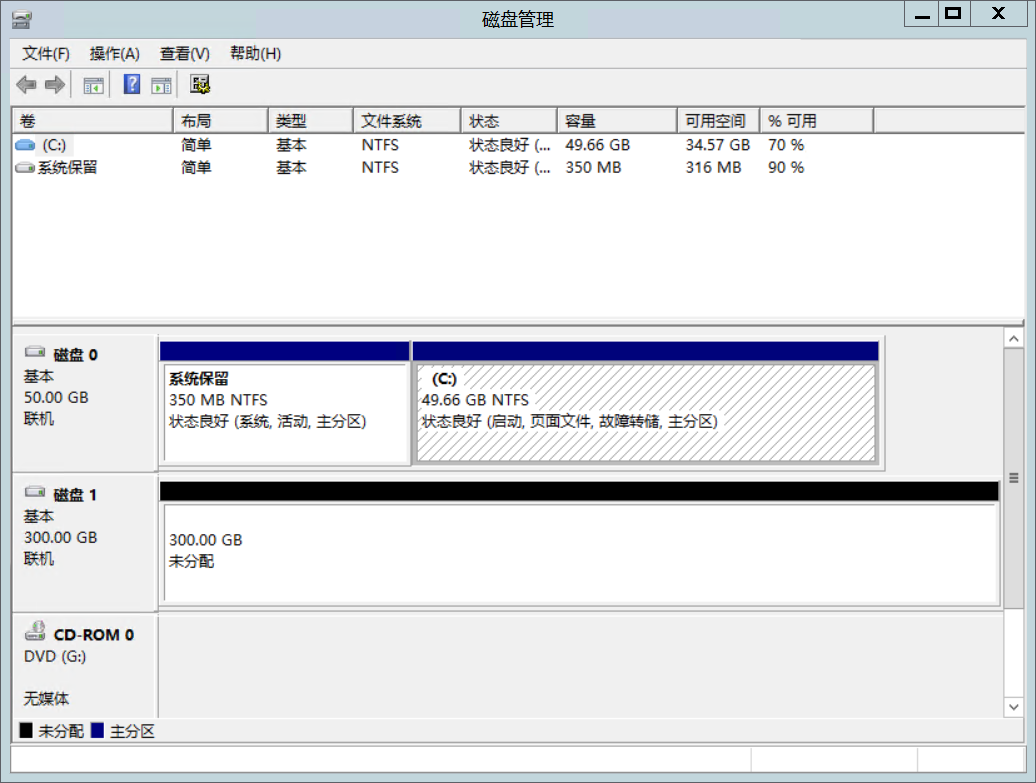
使用远程连接工具，通过运维工作组提供的IP地址、用户名和密码信息连接至虚拟机。与虚拟机连接后，核对虚拟机配置与申请的硬件配置是否一致、内容包括处理器、内存、磁盘容量、内部网和外部网（如果有）的IP地址和端口映射等。

虚拟机的初始状态如下：

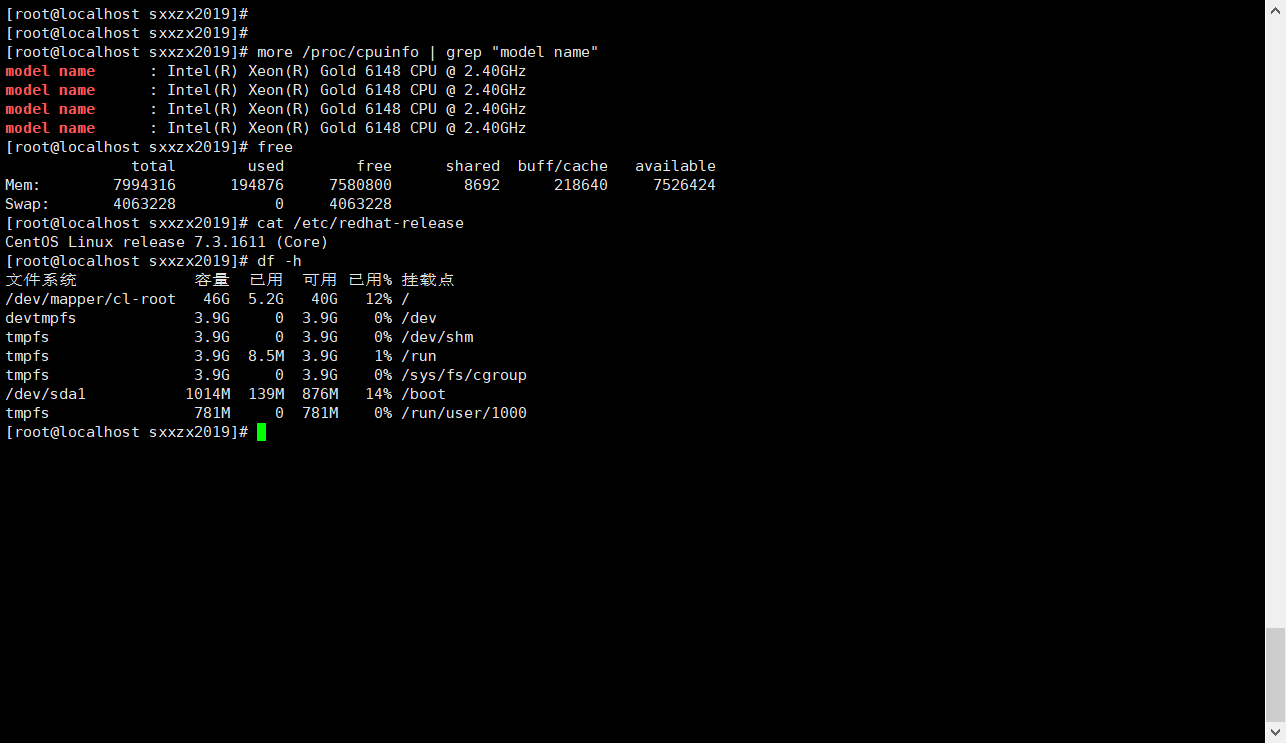
|  |  |
| --- | --- |
| 虚拟机配置 | 操作系统类型和版本：与资源申请表相同  处理器和内存：与资源申请表相同  磁盘：与资源申请表相同，按照系统盘+附加盘的方式提供  IP：内部IP地址由运维工作组分配，内部地址与公网IP的映射已配置 |
| 防火墙 | 操作系统的防火墙为开启状态 |
| 杀病毒软件 | 已安装企业版杀病毒软件 |
| 安全加固 | 已按照等保要求进行了安全加固 |
| 时间服务 | 虚拟机与物理主机的时间未同步，与时间服务器未同步 |
| 附加软件 | 操作系统按照通用方式安装，未安装附加软件 |

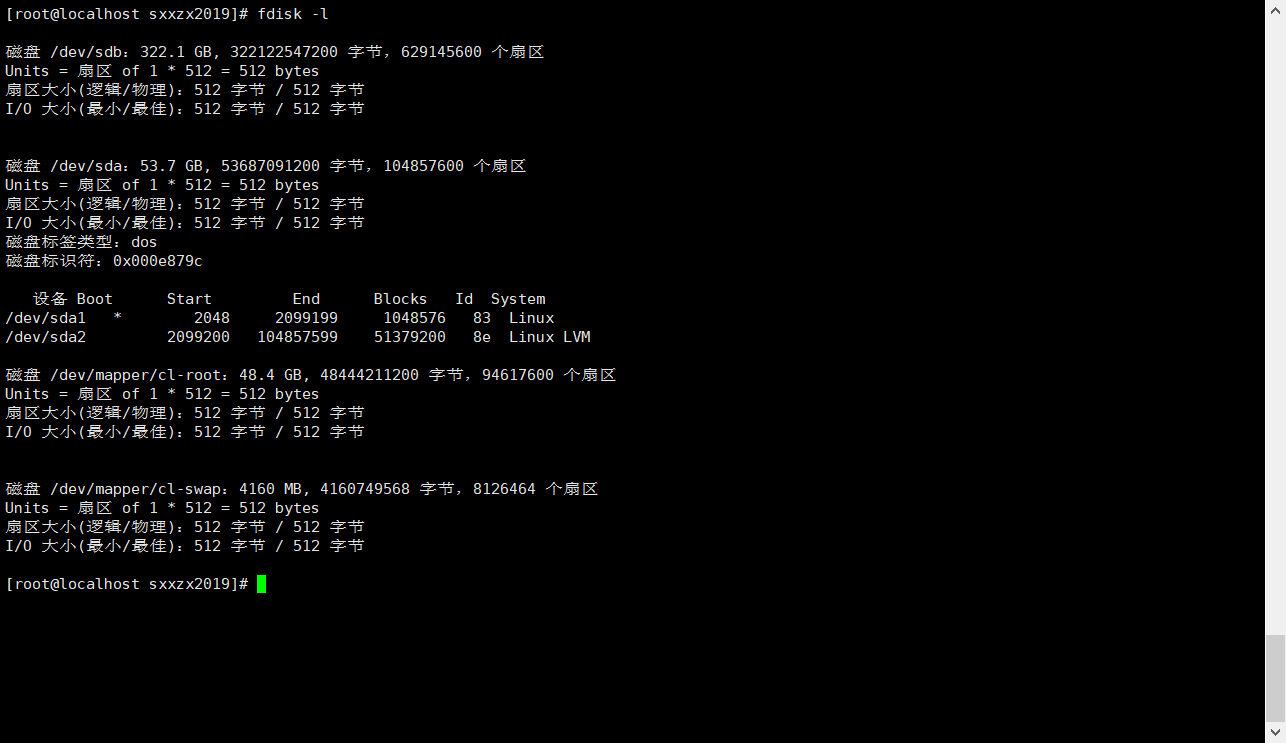
Windows：





CentOS：

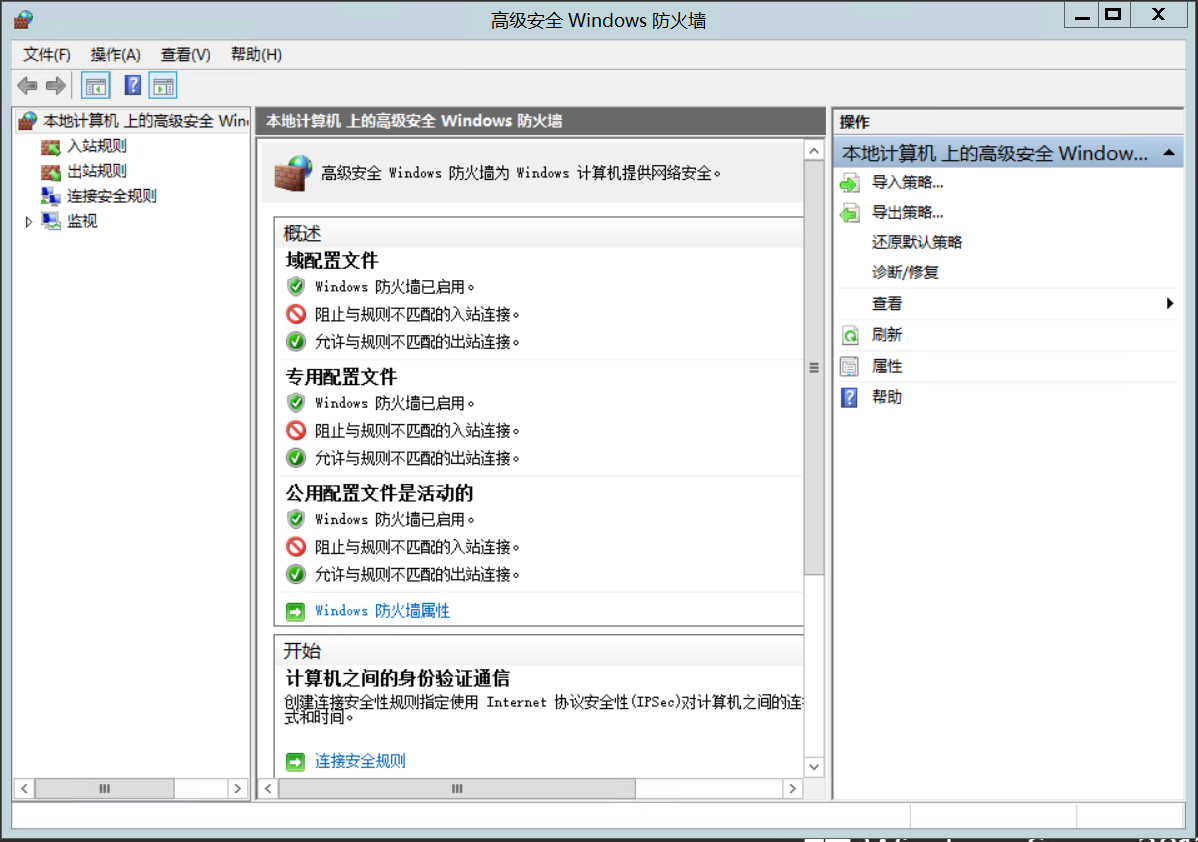




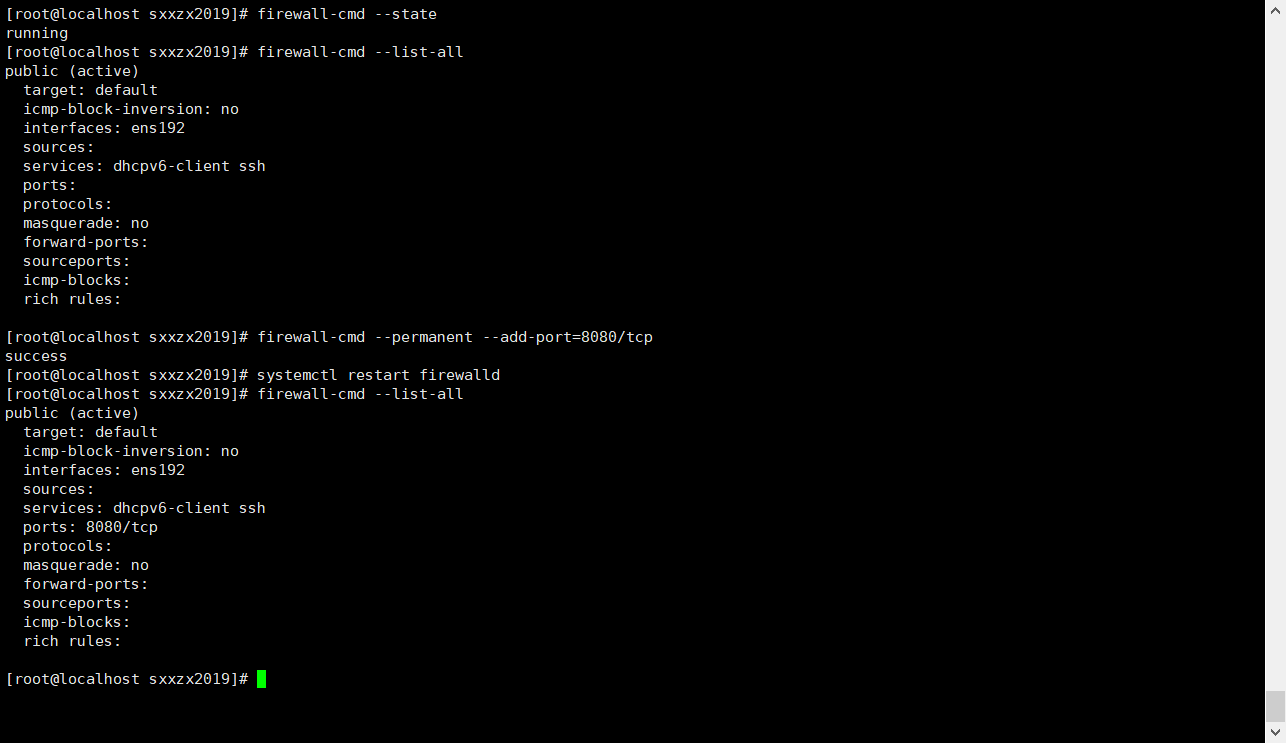
## 查看和更改防火墙配置

操作系统的防火墙为开启状态，虚拟机使用人员请根据业务需要，自行开放相应端口。

Windows：进入“控制面板”的“防火墙”配置界面，使用防火墙“高级设置”，配置防火墙出站与入站规则。



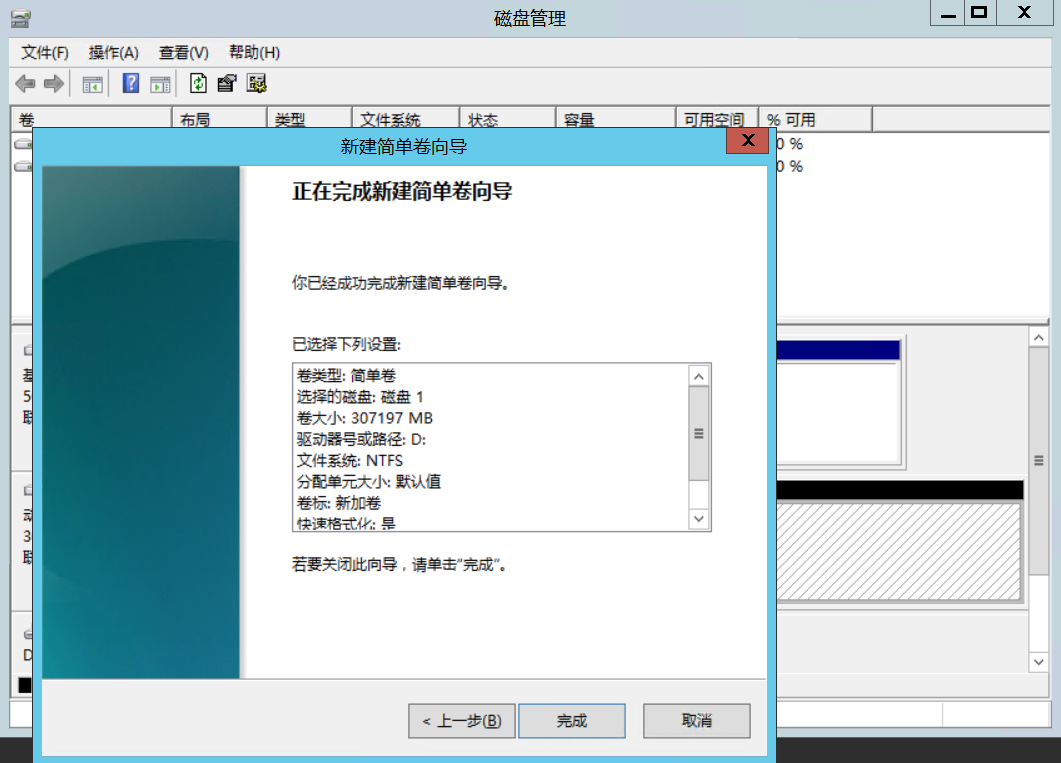
CentOS：CentOS6使用iptables、CentOS7使用firewall-cmd查看和配置防火墙。



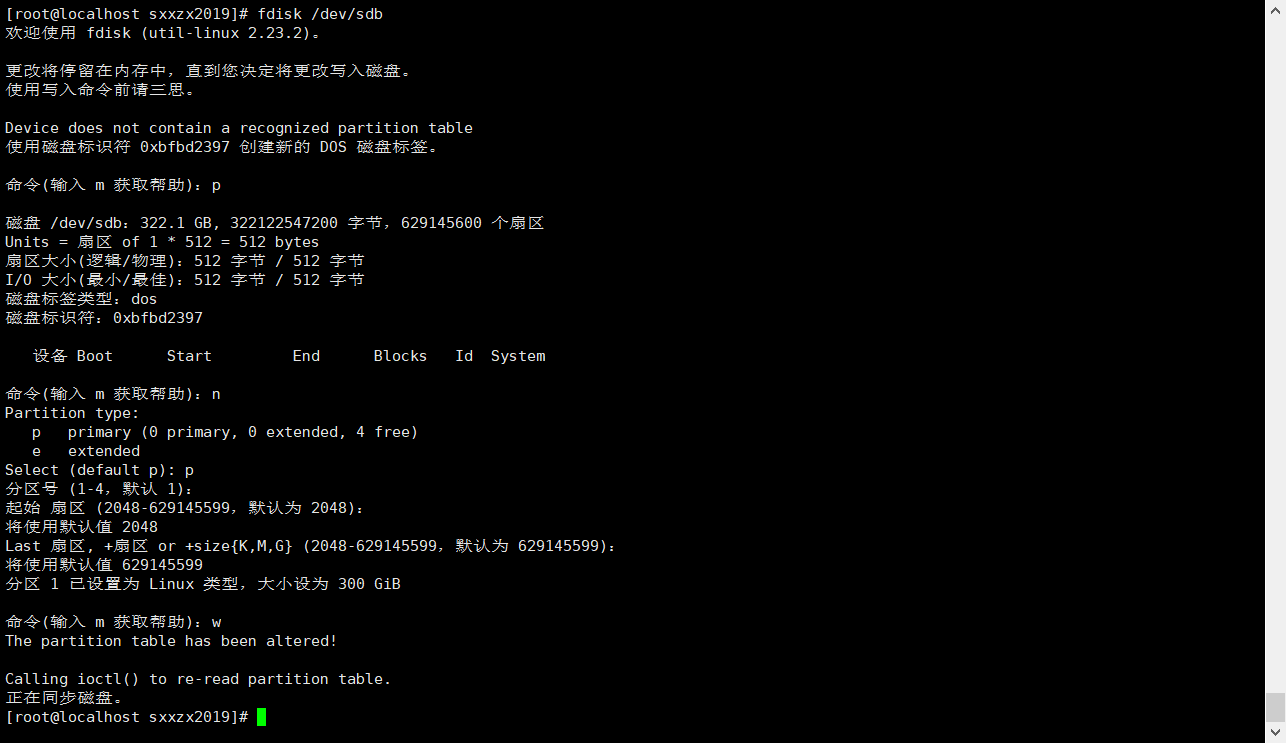
## 查看和更改磁盘配置

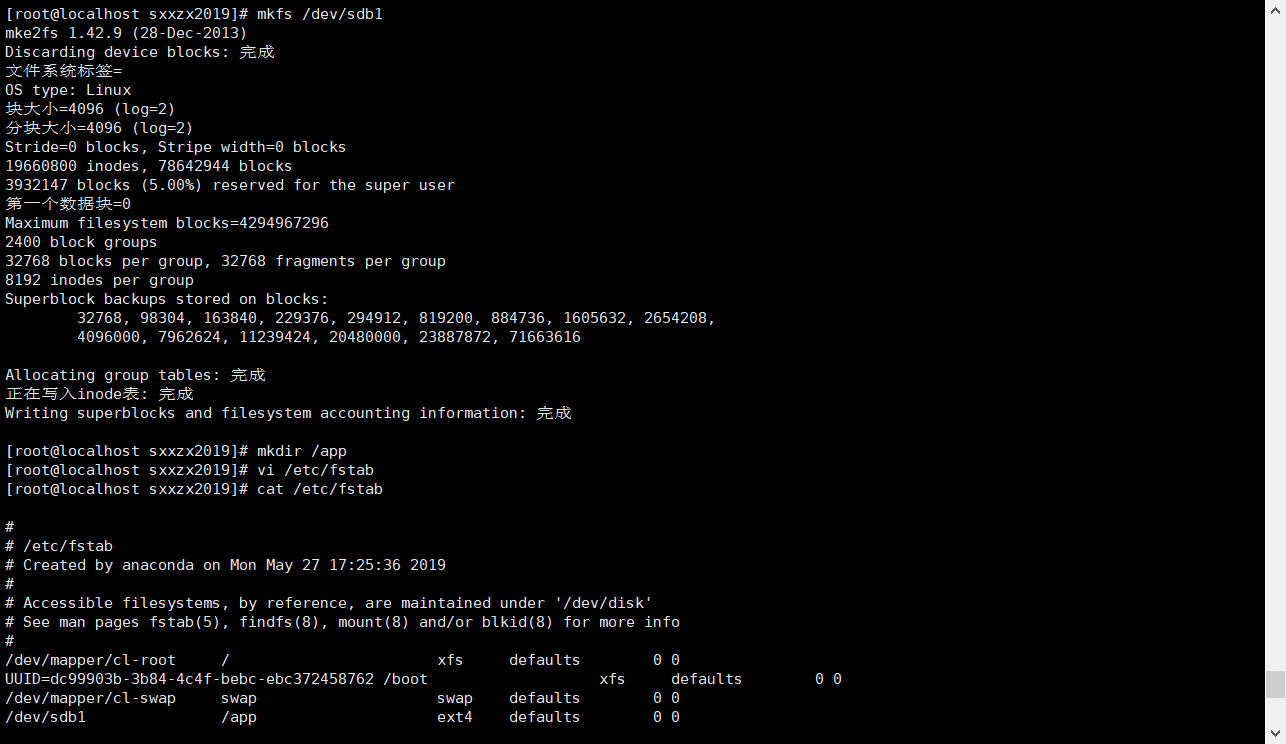
虚拟机的磁盘以系统盘+数据盘的方式提供。系统盘的容量较小，因此不建议使用系统盘存放应用程序与数据，建议将应用程序和数据存放在数据盘中。

Windows：在“磁盘管理”中，新建简单卷，并根据向导完成简单卷的创建，将应用程序与本地数据存放在新创建的卷中。



CentOS：使用fdisk、mkfs、mount等命令创建和挂载数据盘，并将挂载信息写入/etc/fstab文件中，防止虚拟机重启后挂载失效。



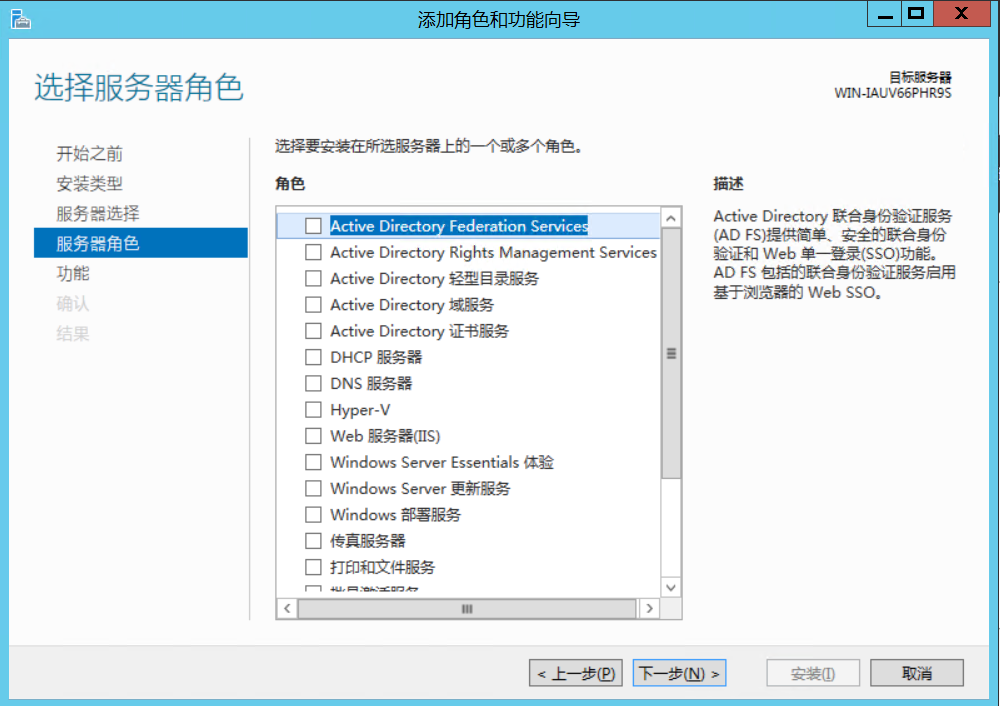




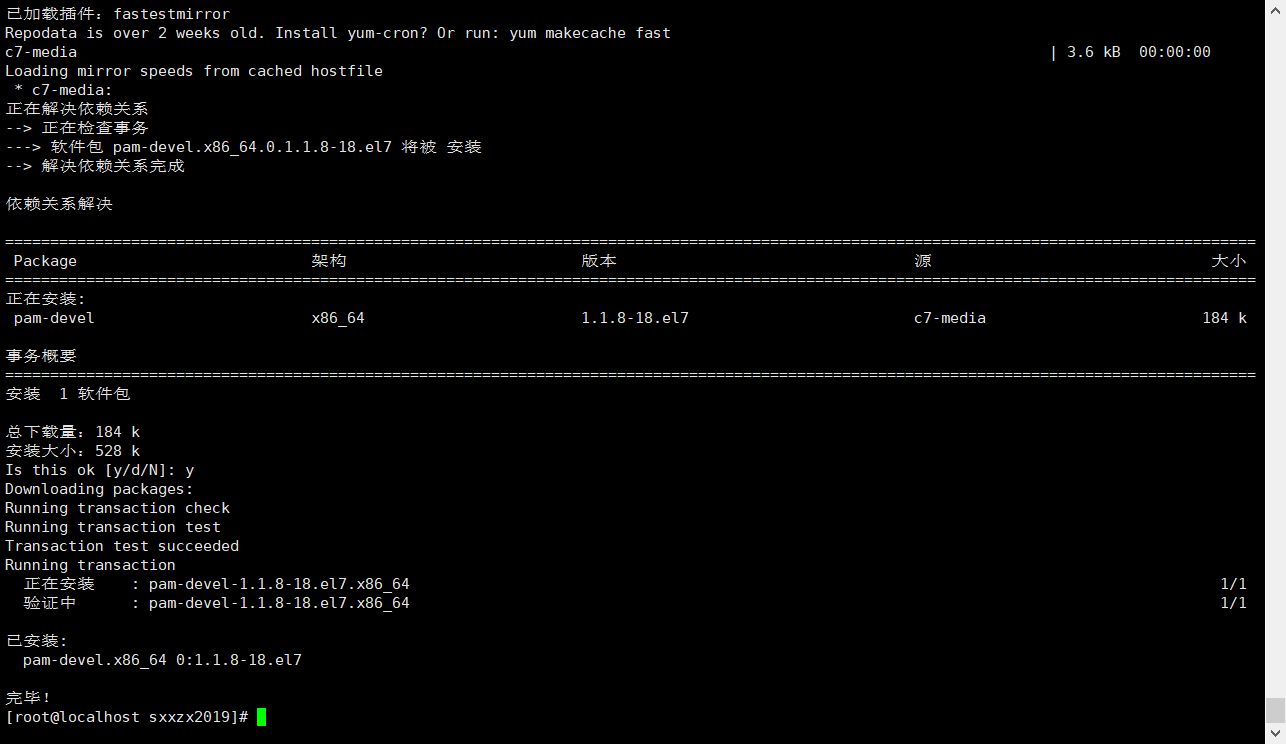
## 检查和安装必要的组件

虚拟机使用人员请根据业务需要，自行安装必要的组件。

Windows：使用“服务器管理器”的“添加角色与功能”选项添加所需组件；组件安装过程如需加载操作系统光盘，请与运维工作组联系，运维工作组联系方式见《附件1：运维工作组联系方式》。



CentOS：虚拟机已配置本地YUM源，可直接安装所需的组件。



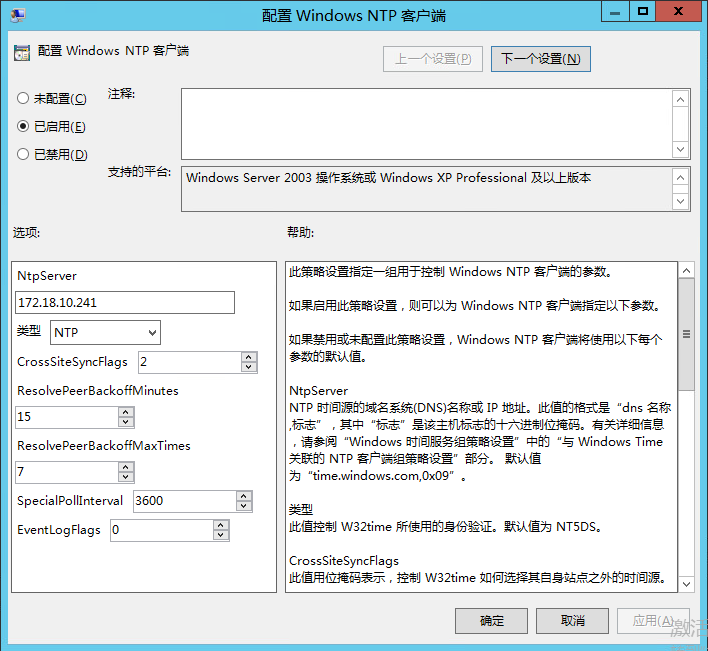
## 与NTP服务器时间同步

在政务外网区和互联网区各有一台NTP Server，虚拟机使用人员请根据业务需要，选择使用本机时间或者同步NTP Server的时间。

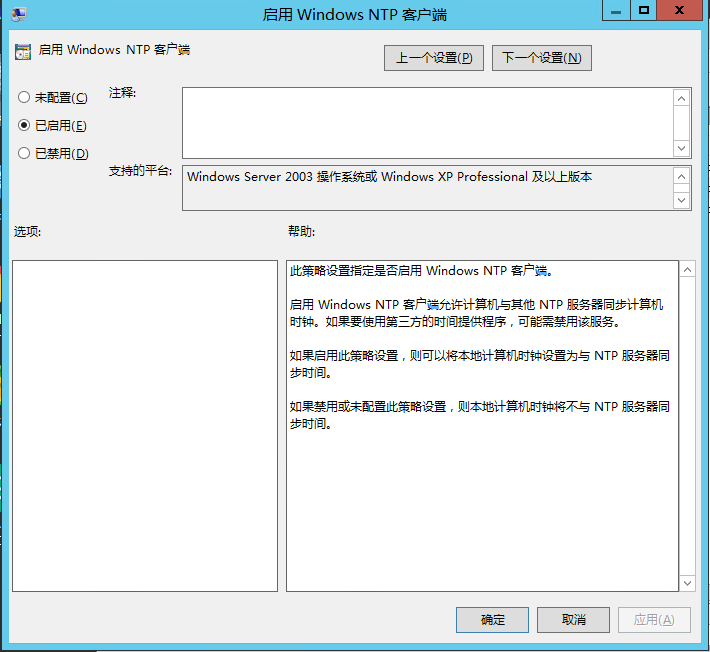
**政务外网区NTP Server：172.18.10.241**

**互联网区NTP Server：10.100.5.26**

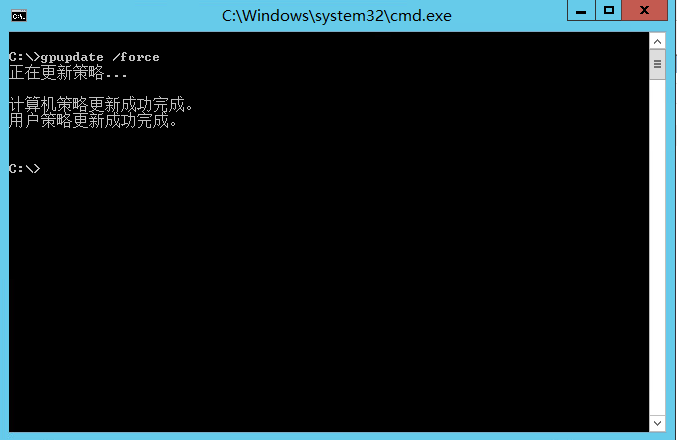
**Windows：运行gpedit.msc，打开组策略管理器，路径“计算机配置\管理模板\系统\windows 时间服务\时间提供程序\配置Windows NTP客户端”。**



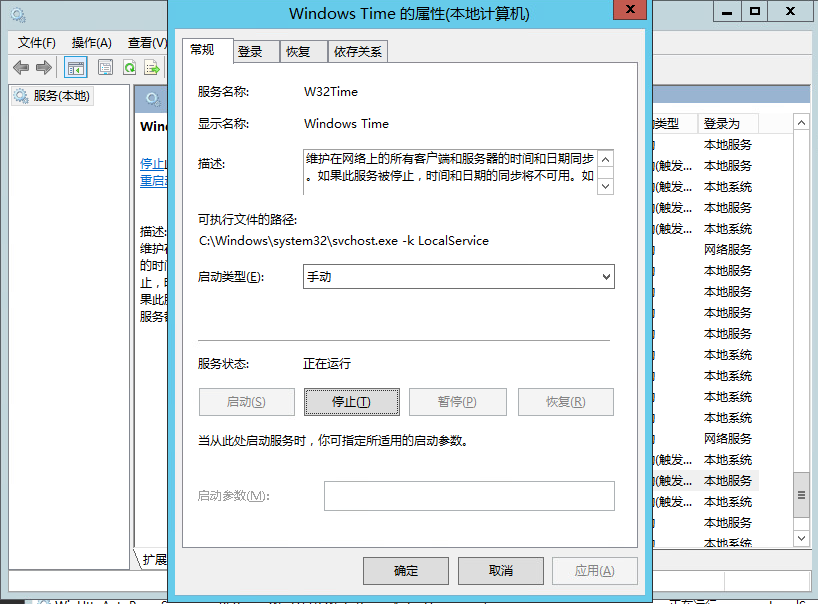
选择“启用Windows NTP客户端”并启用。



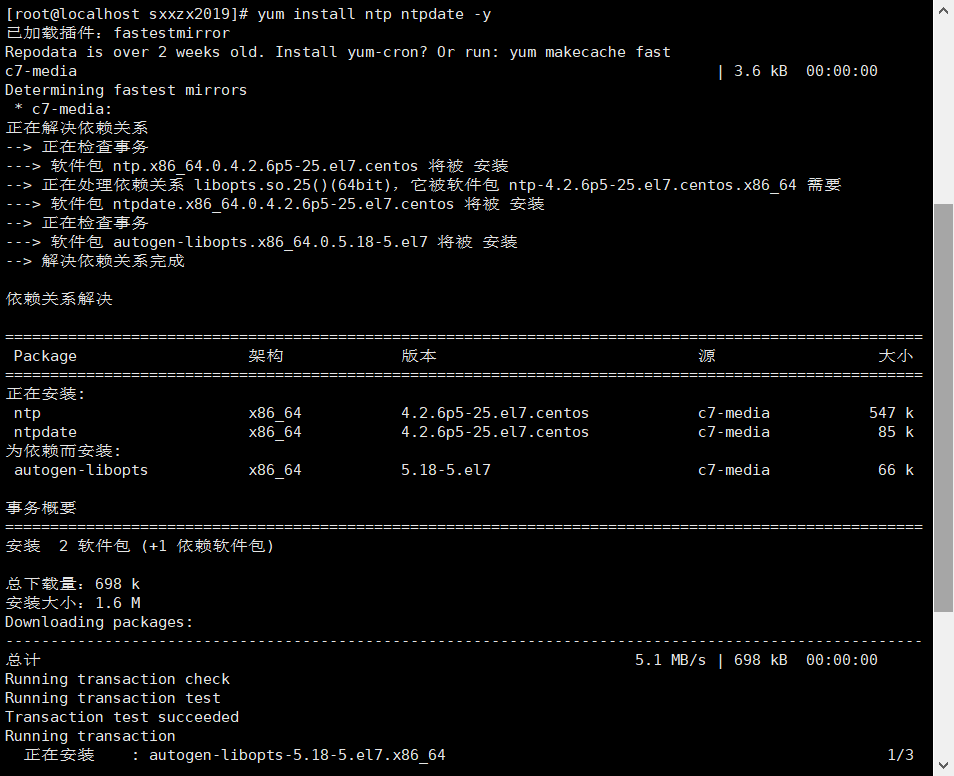
执行命令gpupdate /force，更新组策略。



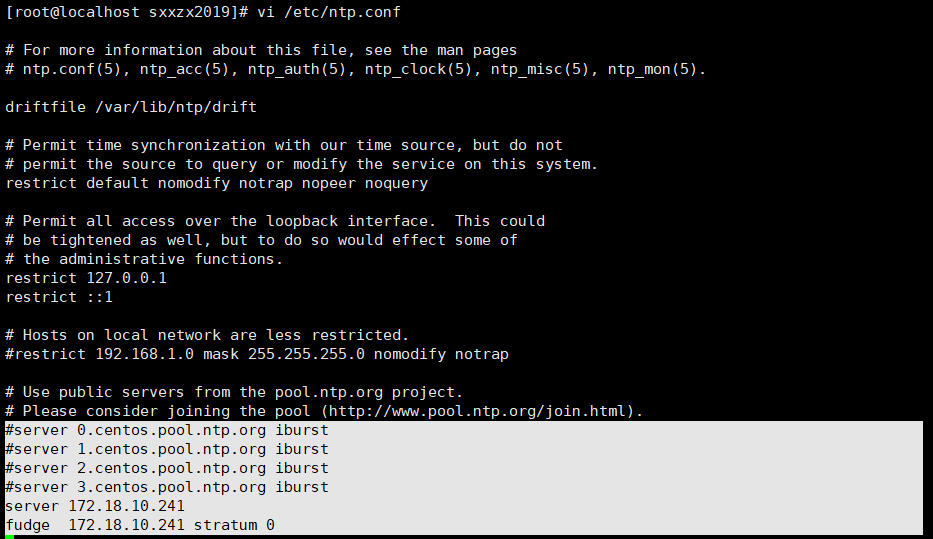
启动W32time服务。



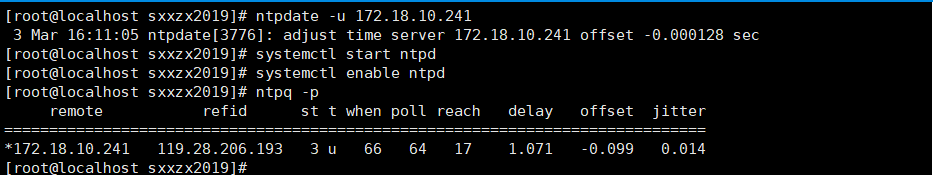
**CentOS：运行yum install ntp ntpdate -y，安装所需软件。**



vi /etc/ntp.conf，按照白色标注的示例进行更改。



启动ntp服务：systemctl start ntpd；并设置开机自启动：systemctl enable ntpd。



## 安装应用软件

虚拟机使用人员请根据业务需要，自行安装所需应用软件，应用软件和数据建议存放在数据磁盘中。

# 数据库使用指南

## ODA IP地址

省信息中心政务外网区现有ODA数据库机 X6-2和X7-2各一台，互联网区现有ODA数据库机 X6-2 一台。

### 政务外网区ODA X6-2 IP地址

Private IP：172.18.10.201 172.18.10.202

VIP：172.18.10.203 172.18.10.204

SCAN IP:172.18.10.205

### 政务外网区ODA X7-2 IP地址

Private IP：172.18.10.211 172.18.10.212

VIP：172.18.10.213 172.18.10.214

SCAN IP:172.18.10.215

### 互联网区ODA X6-2 IP地址

Private IP：10.100.10.201 10.100.10.202

VIP：10.100.10.203 10.100.10.204

SCAN IP: 10.100.10.205

## ODA中创建用户和表

**应用数据请勿存放在SYSTEM表空间。如对数据库创建用户和表的操作有疑问，请与运维工作组联系，运维工作组联系方式见《附件1：运维工作组联系方式》**

使用非system表空间创建用户和表的具体操作如下：

### 创建用户

创建用户时，需提前建立自己的表空间，并且创建用户时不要指定默认表空间为SYSTEM表空间，而是要指定为自己的表空间。

CREATE USER test

IDENTIFIED BY "test321"

DEFAULT TABLESPACE test ---指定表空间

TEMPORARY TABLESPACE TEMP --指定临时表空间

PROFILE DEFAULT---指定概要文件

quota 100m on test --指定配额

ACCOUNT UNLOCK;

### 创建表

创建表时，如果已确认，自己的用户默认表空间不是SYSTEM,那么建表时可以不指定表空间；如果不确定，请在建表时指定自己的表空间名称，如下：

CREATE TABLE test.DEPT

(

DEPTNO NUMBER(2),

DNAME VARCHAR2(14 BYTE),

LOC VARCHAR2(13 BYTE)

)

TABLESPACE test；---------指定test表空间

#### 创建表空间命令：

CREATE TABLESPACE test DATAFILE

'+DATA' SIZE 100M AUTOEXTEND ON NEXT 50M MAXSIZE UNLIMITED；

注：黄色标记为自己数据库数据文件路径。

#### 查询数据库datafile 物理位置：

SQL> show pdbs

CON\_ID CON\_NAME OPEN MODE RESTRICTED

---------- ------------------------------ ---------- ----------

2 PDB$SEED READ ONLY NO

3 ZWFWPTPUB1 READ WRITE NO

4 ZWFWPTPUB2 READ WRITE NO

5 TZXMSPPUB READ WRITE NO

6 ZWZYGXPUB READ WRITE NO

7 TEST READ WRITE NO

8 TESTPDB READ WRITE NO

9 ZXPTPUB READ WRITE NO

10 DHPUB READ WRITE NO

11 SXSZFPT READ WRITE NO

12 SXXYD READ WRITE NO

CON\_ID CON\_NAME OPEN MODE RESTRICTED

---------- ------------------------------ ---------- ----------

13 QZQDXTYY READ WRITE NO

SQL> alter session set container=ZWFWPTPUB1;

Session altered.

SQL> show pdbs

CON\_ID CON\_NAME OPEN MODE RESTRICTED

---------- ------------------------------ ---------- ----------

3 ZWFWPTPUB1 READ WRITE NO

SQL> set linesize 500

SQL> col file\_name for a50

SQL> select file\_name from dba\_data\_files where tablespace\_name='SYSTEM';

FILE\_NAME

--------------------------------------------------

/u02/app/oracle/oradata/datsxipub/sxipub/SXIPUB/5E292CFEFDE84C35E053CA0A640ABB24/datafile/o1\_mf\_system\_f0x1rtl8\_.dbf

黄色标记就是所需数据库的datafile 物理目录，数据文件命名尽量使用 表空间名称+序号方式。

# 附件1：运维工作组联系方式

|  |  |  |
| --- | --- | --- |
| 职务 | 姓名 | 电话 |
| 运维工作组组长 | 魏万军 | 18893118534 |
| VPN技术支持 | 魏家鑫 | 15713981036 |
| 网络/虚拟机技术支持 | 王等强 | 16620075430 |
| 网络/虚拟机技术支持 | 张磊 | 18309220658 |
| 存储技术支持 | 毋果津 | 13060373369 |
| 数据库技术支持 | 张永振 | 13826519358 |