ipa-server搭建及排错之过程

一、服务端配置:

硬件环境: **KVM(4C/8G/100G)**
系统环境: **CentOS-6.5-x86_64-minimal**
软件环境: **Dogtag Certificate System(389 Directory Server/Kerberos KDC with LDAP Backend/Apache for Web Based Services/ ipa_kpasswd/DNS/NTP)**

网络配置**:**

主机名	ipa01.cmccrd.com	ipa02.cmccrd.com	ipa03.cmccrd.com
IP地址	192.168.11.50	192.168.11.51	192.168.11.32
网关	192.168.11.251	192.168.11.251	192.168.11.251
DNS	192.168.11.7	192.168.11.7	192.168.11.7
IPTABLES/SELINUX	关闭	关闭	关闭

安装软件:

```
#yum -y install ipa-server
```

执行安装脚本

```
#ipa-server-instal
```

设置ipa服务开机启动状态:

```
#chkconfig ipa on
```

服务端安装日志保存路径: /var/log/ipaserver-install/log

访问方式
http://ipa01.cmccrd.com

防火墙配置: 如需要开启防火墙，请开启以下端口:
tcp 88
udp 88
tcp 464
udp 464
tcp 53
udp 53
udp 123
tcp 389
tcp 636
tcp 80
tcp 443
tcp 7389

二、服务端Replicate配置

1、安装ipa-server软件包

```
[root@ipa02 ~]# yum install ipa-server
```

2、在ipa01上进行replica preparation

```
[root@ipa01 ~]# ipa-replica-prepare —ip-address=192.168.11.51 ipa02.cmccrd.com
```

3、执行完成之后会在/var/lib/ipa/下生成ipa02所需IPA Multimaster Replication的gpg文件，然后将它拷贝到ipa02

```
[root@ipa01 ~]# scp /var/lib/ipa/replica-info-ipa02.cmccrd.com.gpg ipa02.cmccrd.com:/var/lib/ipa/
```

4、在ipa02上执行如下命令进行ipa-replica的安装并配置ca和dns-forwarder

```
[root@ipa02 ~]# ipa-replica-install /var/lib/ipa/replica-info-ipa02.cmccrd.com.gpg
输入DM password:
输入ipa管理员密码:
```

配置完成后，可以通过如下命令查看ipa-replica的服务器列表

```
[root@ipa01 ~]# ipa-replica-manage list
ipa01.cmccrd.com: master
ipa02.cmccrd.com: master
```

三、IPA客户端配置:

安装软件包: #yum -y install ipa-client
执行安装脚本: #ipa-client-install

非交互式安装方法：/usr/sbin/ipa-client-install --domain=cmccrd.com --server=ipa01.cmccrd.com --enable-dns-updates --mkhomedir -p admin -w xxxxx --realm=CMCCRD.COM —unattended

四、常见问题

常见问题	故障级别	故障描述	解决办法	影响范围
登录	严重	ipa账号无法登录	启动sssd服务	当前主机
家目录	严重	用户无home目录	启动oddjobd服务，并—enablemkhomedir	当前主机
sudo	严重	用户不能sudo	ipa-client-install脚本不提供sudo的自动配置，因此需要手动修改配置文件完成/etc/sssd/sssd.conf /etc/nsswitch.conf /etc/sudo-ldap.conf。在/etc/sudo-ldap.conf中开启debug排错，请注意您所属角色是否拥有您所使用命令的执行权限。	当前主机
启动失败	灾难	ipa服务启动失败	重启后dse.ldif文件丢失，原因目录服务非法关闭	所有主机
web登录失败	严重	web页面用户无法登录	注意服务器时间是否正确，NTP问题	所有主机

五、外部DNS服务的配置：

如果在搭建过程中选择使用外部的DNS服务器，那么你需要在您的dns服务器中增加如下资源解析记录：

```
$ORIGIN cmccrd.com.
ipa01              IN A    192.168.11.50
                  TXT     "kvm:kvm02.cmccrd.com"
ipa02              IN A    192.168.11.51
                  TXT     "kvm:kvm13.cmccrd.com"
;
; ldap servers
_ldap._tcp          IN SRV 0 100 389       ipa01
_ldap._tcp          IN SRV 0 100 389       ipa02

;kerberos realm
_kerberos           IN TXT CMCCRD.COM

; kerberos servers
_kerberos._tcp         IN SRV 0 100 88        ipa01
_kerberos._tcp         IN SRV 0 100 88        ipa02
_kerberos._udp          IN SRV 0 100 88        ipa01
_kerberos._udp          IN SRV 0 100 88        ipa02
_kerberos-master._tcp   IN SRV 0 100 88        ipa01
_kerberos-master._tcp   IN SRV 0 100 88        ipa02
_kerberos-master._udp   IN SRV 0 100 88        ipa01
_kerberos-master._udp   IN SRV 0 100 88        ipa02
_kpasswd._tcp          IN SRV 0 100 464       ipa01
_kpasswd._tcp          IN SRV 0 100 464       ipa02
_kpasswd._udp           IN SRV 0 100 464       ipa01
_kpasswd._udp           IN SRV 0 100 464       ipa02

;ntp server
_ntp._udp           IN SRV 0 100 123       ipa01
_ntp._udp           IN SRV 0 100 123       ipa02
```

六、与第三方应用整合的配置：

以jira为例：

```
=== Current user ===
Directory ID: 1
Username: admin
Display name: cmccrd
Email address: admin@cmccrd.com

=== Directories configured ===
Directory ID: 1
Name: JIRA Internal Directory
Active: true
Type: INTERNAL
Created date: Thu Feb 28 11:57:51 CST 2013
Updated date: Thu Feb 28 11:57:51 CST 2013
Allowed operations: [CREATE_GROUP, CREATE_ROLE, CREATE_USER, DELETE_GROUP, DELETE_ROLE, DELETE_USER, UPDATE_GROUP,
UPDATE_GROUP_ATTRIBUTE, UPDATE_ROLE, UPDATE_ROLE_ATTRIBUTE, UPDATE_USER, UPDATE_USER_ATTRIBUTE]
Implementation class: com.atlassian.crowd.directory.InternalDirectory
Encryption type: atlassian-security
Attributes:
    "user_encryption_method": "atlassian-security"

Directory ID: 10000
Name: IPA-SERVER
Active: false
Type: CONNECTOR
Created date: Mon Aug 25 12:02:29 CST 2014
Updated date: Tue Aug 26 10:45:57 CST 2014
Allowed operations: [UPDATE_GROUP_ATTRIBUTE, UPDATE_USER_ATTRIBUTE]
Implementation class: com.atlassian.crowd.directory.OpenLDAPRfc2307
Encryption type: sha
Attributes:
    "autoAddGroups": ""
    "com.atlassian.crowd.directory.sync.currentstartsynctime": "null"
    "com.atlassian.crowd.directory.sync.lastdurationms": "121"
    "com.atlassian.crowd.directory.sync.laststartsynctime": "1409021130522"
    "crowd.sync.incremental.enabled": "true"
    "directory.cache.synchronise.interval": "3600"
    "ldap.basedn": "dc=cmccrd,dc=com"
    "ldap.connection.timeout": "10000"
    "ldap.external.id": "entryUUID"
    "ldap.group.description": "groupofnames"
    "ldap.group.dn": ""
    "ldap.group.filter": "(objectclass=posixgroup)"
    "ldap.group.name": "uid"
    "ldap.group.objectclass": "posixgroup"
    "ldap.group.usernames": "uniqueMember"
    "ldap.local.groups": "false"
    "ldap.nestedgroups.disabled": "true"
    "ldap.pagedresults": "false"
    "ldap.pagedresults.size": "1000"
    "ldap.password": ********
    "ldap.pool.initsize": "null"
    "ldap.pool.maxsize": "null"
    "ldap.pool.prefsize": "null"
    "ldap.pool.timeout": "0"
    "ldap.propogate.changes": "false"
    "ldap.read.timeout": "120000"
    "ldap.referral": "false"
    "ldap.relaxed.dn.standardisation": "true"
    "ldap.roles.disabled": "true"
    "ldap.search.timelimit": "60000"
    "ldap.secure": "false"
    "ldap.url": "ldap://ipa01.cmccrd.com:389"
    "ldap.user.displayname": "Administrator"
    "ldap.user.dn": ""
    "ldap.user.email": "Administrator"
    "ldap.user.encryption": "sha"
    "ldap.user.filter": "(objectclass=posixaccount)"
    "ldap.user.firstname": "givenName"
    "ldap.user.group": "memberOf"
    "ldap.user.lastname": "sn"
    "ldap.user.objectclass": "posixaccount"
    "ldap.user.password": "userpassword"
    "ldap.user.username": "cn"
    "ldap.user.username.rdn": "cn"
    "ldap.userdn": "uid=sherwinwang,cn=users,cn=accounts,dc=cmccrd,dc=com"
    "ldap.usermembership.use": "false"
    "ldap.usermembership.use.for.groups": "false"
    "localUserStatusEnabled": "false"

Directory ID: 10001
Name: IPA-SERVER
Active: true
Type: CONNECTOR
Created date: Mon Aug 25 13:07:30 CST 2014
Updated date: Tue Aug 26 11:04:24 CST 2014
Allowed operations: [CREATE_GROUP, DELETE_GROUP, UPDATE_GROUP, UPDATE_GROUP_ATTRIBUTE, UPDATE_USER_ATTRIBUTE]
Implementation class: com.atlassian.crowd.directory.GenericLDAP
Encryption type: ssha
Attributes:
    "autoAddGroups": "jira-users"
    "com.atlassian.crowd.directory.sync.currentstartsynctime": "null"
    "com.atlassian.crowd.directory.sync.lastdurationms": "183"
    "com.atlassian.crowd.directory.sync.laststartsynctime": "1409021815869"
    "crowd.sync.incremental.enabled": "true"
    "directory.cache.synchronise.interval": "3600"
    "ldap.basedn": "cn=users,cn=accounts,dc=cmccrd,dc=com"
    "ldap.connection.timeout": "10000"
    "ldap.external.id": "entryUUID"
    "ldap.group.description": "description"
    "ldap.group.dn": ""
```

```
"ldap.group.filter": "(objectclass=groupOfUniqueNames)"
"ldap.group.name": "cn"
"ldap.group.objectclass": "groupOfUniqueNames"
"ldap.group.usernames": "uniqueMember"
"ldap.local.groups": "true"
"ldap.nestedgroups.disabled": "true"
"ldap.pagedresults": "false"
"ldap.pagedresults.size": "1000"
"ldap.password": ********
"ldap.pool.initsize": "null"
"ldap.pool.maxsize": "null"
"ldap.pool.prefsize": "null"
"ldap.pool.timeout": "0"
"ldap.propogate.changes": "false"
"ldap.read.timeout": "120000"
"ldap.referral": "false"
"ldap.relaxed.dn.standardisation": "false"
"ldap.roles.disabled": "true"
"ldap.search.timelimit": "60000"
"ldap.secure": "false"
"ldap.url": "ldap://ipa01.cmccrd.com:389"
"ldap.user.displayname": "displayName"
"ldap.user.dn": ""
"ldap.user.email": "mail"
"ldap.user.encryption": "ssha"
"ldap.user.filter": "(objectclass=inetorgperson)"
"ldap.user.firstname": "givenName"
"ldap.user.group": "memberOf"
"ldap.user.lastname": "sn"
"ldap.user.objectclass": "inetorgperson"
"ldap.user.password": "userPassword"
"ldap.user.username": "uid"
"ldap.user.username.rdn": "uid"
"ldap.userdn": "uid=admin,cn=users,cn=accounts,dc=cmccrd,dc=com"
"ldap.usermembership.use": "false"
"ldap.usermembership.use.for.groups": "false"
"localUserStatusEnabled": "false"
```