IT NPC

首页　　　　IDC业务　　　　站长资讯　　　　站长工具

当前位置： 首页 > 站长资讯 > 建站　　　　　投稿　　　订阅

请输入需要搜索的内容

1	linux的学习	4	高防服务器
2	编程学习入门	5	linux运维
3	环保集成墙面	6	大数据学习

资讯分类　　　　工具分类

SEO工　　　　IP工具

网络辅　　　　远程控

网站源　　　　制

Linux与云计算——第二阶段Linux服务器架设 第六章：目录Directory服务器架设—FreeIPA

时间：2016-08-02 16:12:11　来源：11830455　编辑：涛涛　点击：46

A-　A+

数据分析培训班　数据仓库 olap　　大数据分析　ios工程师月薪

Linux与云计算——第二阶段Linux服务器架设

第六章：目录Directory服务器架设—FreeIPA

1 FreeIPA 配置FreeIPA服务器

```
    Configure IPA Server to share users' account in your local network.
[1] Install FreeIPA.
[root@dlp ~]# yum -y install ipa-server ipa-server-dns bind bind-dyndb-ldap
[2] Setup FreeIPA Server.
[root@dlp ~]# vi /etc/hosts
# add own IP
   10.0.0.30      dlp.srv.world dlp

[root@dlp ~]# ipa-server-install --setup-dns
The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will set up the IPA Server.

This includes:
    * Configure a stand-alone CA (dogtag) for certificate management
    * Configure the Network Time Daemon (ntpd)
    * Create and configure an instance of Directory Server
    * Create and configure a Kerberos Key Distribution Center (KDC)
    * Configure Apache (httpd)

To accept the default shown in brackets, press the Enter key.

# setup DNS (existing BIND settings is over-written)
Existing BIND configuration detected, overwrite? [no]: yes
Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
```

环保集成墙面

常用在线工具　　　　常用工具下载

收录提交大全　　　　　网站综合排行榜
网站综合排行榜　　　　网站综合排行榜
网站综合排行榜　　　　网站综合排行榜
网站综合排行榜　　　　网站综合排行榜

广告位

热门内容　　　　推荐信息

1　虚幻4视频笔记002：精简StarterConte
2　8.23_Linux软件包管理之编译程序包
3　浅谈JNDI导入两个同名不同路径jar
4　smb协议详解和samba服务的配置
5　Corosync Pacemaker 高可用 Mariad
6　nagios部署监控多台client
7　Activity启动流程
8　MySql忘记root密码的解决方法
9　Java集合之Map接口

```
Example: master.example.com.

# confirm the hostname and Enter
Server host name [dlp.srv.world]:

The domain name has been determined based on the host name.

# confirm the domain name and Enter
Please confirm the domain name [srv.world]:

The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.

# confirm realm name and Enter
Please provide a realm name [SRV.WORLD]:
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

# Directory Manager's password
Directory Manager password:
Password (confirm):

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.

# IPA admin's password
IPA admin password:
Password (confirm):

# answer with yes or no for setting DNS forwarder
Do you want to configure DNS forwarders? [yes]:
Enter the IP address of DNS forwarder to use, or press Enter to finish.
# specify DNS forwarder's IP if you set DNS forwarder
Enter IP address for a DNS forwarder: 10.0.0.10
DNS forwarder 10.0.0.10 added
# Enter with empty if DNS forwarder is OK
Enter IP address for a DNS forwarder:
# answer with yes or no for setting reverse zone
Do you want to configure the reverse zone? [yes]:
# reverse zone name if you set reverse zone
Please specify the reverse zone name [0.0.10.in-addr.arpa.]:

The IPA Master Server will be configured with:
Hostname:          dlp.srv.world
IP address:         10.0.0.30
Domain name:       srv.world
Realm name:        SRV.WORLD

BIND DNS server will be configured to serve IPA domain with:
Forwarders:        10.0.0.10
Reverse zone:     0.0.10.in-addr.arpa.

# confirm settings and proceed with "yes"
Continue to configure the system with these values? [no]: yes

The following operations may take some minutes to complete.
Please wait until the prompt is returned.

Configuring NTP daemon (ntpd)
...
...
...
==================================================================
Setup complete

Next steps:
```

今周排行　本月排行　本季排行

```
                1. You must make sure these network ports are open:
                                TCP Ports:
                                    * 80, 443: HTTP/HTTPS
                                    * 389, 636: LDAP/LDAPS
                                    * 88, 464: kerberos
                                UDP Ports:
                                    * 88, 464: kerberos
                                    * 123: ntp

                2. You can now obtain a kerberos ticket using the command: 'kinit
admin'
                        This ticket will allow you to use the IPA tools (e.g., ipa user-
add)
                        and the web user interface.

Be sure to back up the CA certificate stored in /root/cacert.p12
This file is required to create replicas. The password for this
file is the Directory Manager password
[3] Get Kerberos tickets and change default shell.
[root@dlp ~]# kinit admin
Password for admin@SRV.WORLD:# IPA admin password
[root@dlp ~]# klist # confirm
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@SRV.WORLD

Valid starting          Expires                     Service principal
03/21/2015 14:25:53   03/24/2015 14:25:50    krbtgt/SRV.WORLD@SRV.WORLD

[root@dlp ~]# ipa config-mod --defaultshell=/bin/bash
    Maximum username length: 32
    Home directory base: /home
    Default shell: /bin/bash
    Default users group: ipausers
    Default e-mail domain: srv.world
    Search time limit: 2
    Search size limit: 100
    User search fields: uid,givenname,sn,telephonenumber,ou,title
    Group search fields: cn,description
    Enable migration mode: FALSE
    Certificate Subject base: O=SRV.WORLD
    Password Expiration Notification (days): 4
    Password plugin features: AllowNThash
    SELinux user map order: guest_u:s0$xguest_u:s0$user_u:s0$staff_u:s0-
s0:c0.c1023$unconfined_u:s0-s0:c0.c1023
    Default SELinux user: unconfined_u:s0-s0:c0.c1023
    Default PAC types: MS-PAC
[4] If Firewalld is running, allow FreeIPA services.
[root@dlp ~]# firewall-cmd --add-service={ssh,dns,freeipa-ldap,freeipa-ldaps} --
permanent
success
[root@dlp ~]# firewall-cmd --reload
Success
```

2 增加用户账户

```
    Add User Accounts on FreeIPA Server.
[1] Add a user. The password set on here is required to change at initial login.
[root@dlp ~]# ipa user-add cent --first=CentOS --last=Linux --password
Password:# set password
Enter Password again to verify:
-----------------
Added user "cent"
-----------------
    User login: cent
    First name: CentOS
    Last name: Linux
    Full name: CentOS Linux
    Display name: CentOS Linux
    Initials: CL
    Home directory: /home/cent
```

```
            GECOS field: CentOS Linux
            Login shell: /bin/bash
            Kerberos principal: cent@SRV.WORLD
            Email address: cent@srv.world
            UID: 1219600001
            GID: 1219600001
            Password: True
            Kerberos keys available: True

# confirm
[root@dlp ~]# ipa user-find cent
--------------
1 user matched
--------------
        User login: cent
        First name: CentOS
        Last name: Linux
        Home directory: /home/cent
        Login shell: /bin/bash
        Email address: cent@srv.world
        UID: 1219600001
        GID: 1219600001
        Account disabled: False
        Password: True
        Kerberos keys available: True
----------------------------
Number of entries returned 1
```

[2] Add Existing local Users to IPA Directory (set the same password with the username on this example, but it is required to change at initial login)

```
[root@dlp ~]# vi ipauser.sh
# extract local users who have 1000-9999 digit UID
# this is an example
#!/bin/bash

for line in `grep "x:[1-9][0-9][0-9][0-9]:" /etc/passwd`
do
        USER=`echo $line | cut -d: -f1`
        FIRST=`echo $line | cut -d: -f5 | awk {'print $1'}`
        LAST=`echo $line | cut -d: -f5 | awk {'print $2'}`

        [ ! "$FIRST" ] && FIRST=$USER
        [ ! "$LAST" ] && LAST=$USER

        echo $USER | ipa user-add $USER --first=$FIRST --last=$LAST --password
done
[root@dlp ~]# sh ipauser.sh
------------------
Added user "redhat"
------------------
        User login: redhat
        First name: redhat
        Last name: redhat
        Full name: redhat redhat
        Display name: redhat redhat
        Initials: rr
        Home directory: /home/redhat
        GECOS field: redhat redhat
        Login shell: /bin/bash
        Kerberos principal: redhat@SRV.WORLD
        Email address: redhat@srv.world
        UID: 1219600003
        GID: 1219600003
        Password: True
        Kerberos keys available: True
------------------
Added user "ubuntu"
------------------
        User login: ubuntu
        First name: ubuntu
```

```
    Last name: ubuntu
    Full name: ubuntu ubuntu
    Display name: ubuntu ubuntu
    Initials: uu
    Home directory: /home/ubuntu
    GECOS field: ubuntu ubuntu
    Login shell: /bin/bash
    Kerberos principal: ubuntu@SRV.WORLD
    Email address: ubuntu@srv.world
    UID: 1219600004
    GID: 1219600004
    Password: True
    Kerberos keys available: True
```

3 配置FreeIPA客户端

    Configure FreeIPA Client to connect to FreeIPA Server.
[1] Add DNS entry for FreeIPA client on FreeIPA server first.

```
# ipa dnsrecord-add [domain name] [record name] [record type] [record]
[root@dlp ~]# ipa dnsrecord-add srv.world client01 --a-rec 10.0.0.51
    Record name: client01
    A record: 10.0.0.51
```

[2] Install Client tools on FreeIPA Client Host and change DNS settings.

```
[root@client01 ~]# yum -y install ipa-client
[root@client01 ~]# nmcli c modify eno16777736 ipv4.dns 10.0.0.30
[root@client01 ~]# nmcli c down eno16777736; nmcli c up eno16777736
```

[3] Setup as a FreeIPA Client. Sync time with FreeIPA server before it.

```
[root@client01 ~]# ipa-client-install
Discovery was successful!
Hostname: client01.srv.world
Realm: SRV.WORLD
DNS Domain: srv.world
IPA Server: dlp.srv.world
BaseDN: dc=srv,dc=world

# confirm settings and proceed with "yes"
Continue to configure the system with these values? [no]: yes
# answer with admin
User authorized to enroll computers: admin
Synchronizing time with KDC...
Unable to sync time with IPA NTP server, assuming the time is in sync. Please check
that 123 UDP port is opened.
Password for admin@SRV.WORLD:
Successfully retrieved CA cert
        Subject:        CN=Certificate Authority,O=SRV.WORLD
        Issuer:         CN=Certificate Authority,O=SRV.WORLD
        Valid From:   Fri Mar 20 01:42:15 2015 UTC
        Valid Until: Tue Mar 20 01:42:15 2035 UTC


Enrolled in IPA realm SRV.WORLD
.....
.....
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Client configuration complete.

# configure mkhomedir if you need ( homedirs of users are created at inital login )
[root@client01 ~]# authconfig --enablemkhomedir --update
getsebool: SELinux is disabled
[root@client01 ~]# exit
logout
CentOS Linux 7 (Core)
Kernel 3.10.0-123.20.1.el7.x86_64 on an x86_64
client01 login: redhat # IPA user
Password: # password
Password expired. Change your password now.      # required to change the password when
initial login
Current Password: # current password
New password: # new password
Retype new password:
```

```
Creating home directory for redhat.
[redhat@client01 ~]$ # just logined
```

4 基础配置

[1] Add a FreeIPA user account.

```
[root@dlp ~]# ipa user-add cent --first=CentOS --last=Linux --password
Password:
Enter Password again to verify:
-----------------
Added user "cent"
-----------------
    User login: cent
    First name: CentOS
    Last name: Linux
    Full name: CentOS Linux
    Display name: CentOS Linux
    Initials: CL
    Home directory: /home/cent
    GECOS field: CentOS Linux
    Login shell: /bin/bash
    Kerberos principal: cent@SRV.WORLD
    Email address: cent@srv.world
    UID: 1781800001
    GID: 1781800001
    Password: True
    Kerberos keys available: True
```

[2] Lock or unlock a FreeIPA user.

```
[root@dlp ~]# ipa user-disable cent
---------------------------
Disabled user account "cent"
---------------------------
[root@dlp ~]# ipa user-enable cent
---------------------------
Enabled user account "cent"
---------------------------
```

[3] Search a FreeIPA user.

```
[root@dlp ~]# ipa user-find cent
--------------
1 user matched
--------------
    User login: cent
    First name: CentOS
    Last name: Linux
    Home directory: /home/cent
    Login shell: /bin/bash
    Email address: cent@srv.world
    UID: 1781800001
    GID: 1781800001
    Account disabled: False
    Password: True
    Kerberos keys available: True
----------------------------
Number of entries returned 1
----------------------------

[root@dlp ~]# ipa user-show --raw cent
    uid: cent
    givenname: CentOS
    sn: Linux
    homedirectory: /home/cent
    loginshell: /bin/bash
    mail: cent@srv.world
    uidnumber: 1781800001
    gidnumber: 1781800001
    nsaccountlock: False
    has_password: True
    has_keytab: True
```

[4] Delete a FreeIPA user.

```
[root@dlp ~]# ipa user-del cent
```

```
------------------
Deleted user "cent"
------------------
[5] Add a FreeIPA group.
[root@dlp ~]# ipa group-add --desc='Development Group' development
------------------------
Added group "development"
------------------------
    Group name: development
    Description: Development Group
    GID: 1781800006
[6] Add members in a FreeIPA group.
[root@dlp ~]# ipa group-add-member --users=redhat,ubuntu development
    Group name: development
    Description: Development Group
    GID: 1781800006
    Member users: redhat, ubuntu
------------------------
Number of members added 2
------------------------
[7] Add a group in a FreeIPA group.
[root@dlp ~]# ipa group-add-member --groups=development hiroshima
    Group name: hiroshima
    Description: State Group
    GID: 1781800007
    Member groups: development
------------------------
Number of members added 1
------------------------
[8] Search a FreeIPA group.
[root@dlp ~]# ipa group-find development
---------------
1 group matched
---------------
    Group name: development
    Description: Development Group
    GID: 1781800006
    Member users: redhat, ubuntu
    Member of groups: hiroshima
----------------------------
Number of entries returned 1
----------------------------
[9] Delete a FreeIPA group.
[root@dlp ~]# ipa group-del hiroshima
------------------------
Deleted group "hiroshima"
------------------------
```

5 使用WEB图形化界面

　　It's possible to operate FreeIPA Server on Web Management Console.
[1] Start Web browser on any Client on the same network of FreeIPA Server and access to "https://(FreeIPA server's hostname or IP address)/", then, login form to IPA server is shown like follows. Login with a FreeIPA user. This example use admin user like follows.

[2] Just logined noramlly. It's possible to operate FreeIPA server on GUI easily.

6 FreeIPA Replication

　　Configure FreeIPA Replication.
[1] Install FreeIPA server's tools on the Replica Host and change DNS settings.

```
[root@repl01 ~]# yum -y install ipa-server ipa-server-dns bind bind-dyndb-ldap
# change DNS to FreeIPA server
[root@repl01 ~]# nmcli c modify eno16777736 ipv4.dns 10.0.0.30
[root@repl01 ~]# nmcli c down eno16777736; nmcli c up eno16777736
```
[2] Add DNS entry for Replica Host on FreeIPA server.

```
# ipa dnsrecord-add [domain name] [record name] [record type] [record]
[root@dlp ~]# ipa dnsrecord-add srv.world repl01 --a-rec 10.0.0.61
    Record name: repl01
    A record: 10.0.0.61


[root@dlp ~]# ipa-replica-prepare repl01.srv.world --ip-address 10.0.0.61
Directory Manager (existing master) password:        # Directory Manager password

Preparing replica for repl01.srv.world from dlp.srv.world
Creating SSL certificate for the Directory Server
Creating SSL certificate for the dogtag Directory Server
Creating SSL certificate for the Web Server
Exporting RA certificate
Copying additional files
Finalizing configuration
Packaging replica information into /var/lib/ipa/replica-info-repl01.srv.world.gpg
Adding DNS records for repl01.srv.world
Using reverse zone 0.0.10.in-addr.arpa.


# transfer generated key to Replica Host
[root@dlp ~]# scp /var/lib/ipa/replica-info-repl01.srv.world.gpg
root@repl01.srv.world:/var/lib/ipa/
root@repl01.srv.world's password:
replica-info-repl01.srv.world.gpg 100% 35KB 34.6KB/s 00:00
[3] On FreeIPA server, If Firewalld is running, allow FreeIPA replication service.
[root@dlp ~]# firewall-cmd --add-service=freeipa-replication --permanent
success
[root@dlp ~]# firewall-cmd --reload
Success
[4] On FreeIPA replication Host, If Firewalld is running, allow FreeIPA services.
[root@repl01 ~]# firewall-cmd --add-service={ssh,dns,freeipa-ldap,freeipa-
ldaps,freeipa-replication} --permanent
success
[root@repl01 ~]# firewall-cmd --reload
Success
[5] Setup as a Replica Server on FreeIPA Replica.
    The following example set "--no-forwarders" for DNS, but if you set it, specify
like "--forwarder=x.x.x.x".
[root@repl01 ~]# ipa-replica-install --setup-ca --setup-dns --no-forwarders
/var/lib/ipa/replica-info-repl01.srv.world.gpg
Directory Manager (existing master) password:        # Directory Manager password


Run connection check to master
Check connection from replica to remote master 'dlp.srv.world':
    Directory Service: Unsecure port (389): OK
    Directory Service: Secure port (636): OK
    Kerberos KDC: TCP (88): OK
    Kerberos Kpasswd: TCP (464): OK
    HTTP Server: Unsecure port (80): OK
    HTTP Server: Secure port (443): OK
    PKI-CA: Directory Service port (7389): OK


The following list of ports use UDP protocol and would need to be
checked manually:
    Kerberos KDC: UDP (88): SKIPPED
    Kerberos Kpasswd: UDP (464): SKIPPED


Connection from replica to master is OK.
Start listening on required ports for remote master check
Get credentials to log in to remote master
admin@SRV.WORLD password:          # admin password


Execute check on remote master
.....
.....
Global DNS configuration in LDAP server is empty
You can use 'dnsconfig-mod' command to set global DNS options that
would override settings in local named.conf files
```

```
Restarting the web server
[6] Get Kerberos tickets on Replica Host and make sure it's possible to get datas on
FreeIPA Directory. If possible, it's OK to setup replication settings.
    For FreeIPA Clients, it's not necessarry to set additinal settings, Clients can
continue to authenticate even if a Server is down.
[root@repl01 ~]# kinit admin
Password for admin@SRV.WORLD:          # admin password
[root@repl01 ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@SRV.WORLD

Valid starting              Expires                      Service principal
03/21/2015 15:13:38   03/24/2015 15:13:35   krbtgt/SRV.WORLD@SRV.WORLD

[root@repl01 ~]# ipa user-find
---------------
4 users matched
---------------
    User login: admin
    Last name: Administrator
    Home directory: /home/admin
    Login shell: /bin/bash
    UID: 1219600000
    GID: 1219600000
    Account disabled: False
    Password: True
    Kerberos keys available: True

    User login: cent
    First name: CentOS
    Last name: Linux
    Home directory: /home/cent
    Login shell: /bin/bash
    Email address: cent@srv.world
    UID: 1219600001
    GID: 1219600001
    Account disabled: False
    Password: True
    Kerberos keys available: True
.....
.....
```

喵~!小编每天更新文章,打赏以下，给我家喵星人买罐头吧！

赏

上一篇：Python基础知识（2）——函数
下一篇：Linux下搭建JDK和TOMCAT环境

💰 打赏本站　　💬 踩 1　　⭐ 收藏此文　　分享到：

您看完此文章的心情是

打酱油	震惊	呵呵	赞	鄙视
1人	0人	2人	4人	0人

您看完此刻的感受是？【已有NaN人发表态度

0		0	0	0	0	0	0	0	NaN
狂顶		炒作	膜拜	超囧	鄙视	飘过	感动	纠结	悲痛

相关文章　　　　进入文章频道》

openstack学习笔记八 cinder基础配	2016-07-28
DAY2:CentOS6.8（及7）基础配置项+Linu	
配置mysql replication出错记录	2016-07-26
MySQL5.6 Replication主从复制（读写	2016-07-20
Hibernate基础配置——hibernate.c	2016-07-18
IPSecTunnel mode基础配置　2016-07-06	2016-07-14
4、redis.conf中replication配置项	2016-06-08
MySQL学习笔记之九：MySQL Replicati	2016-06-03

怎样学习编程　　linux红帽认证

马哥linux学习笔记　搭建openvpn服

精彩评论

登录 | 注册

网友提问　　　　已有0人发表评论

暂无评论

当前热门文章　　　　1 2 3

软件工程师待遇

自学平面设计

ios工程师月薪

软件测试工程师

大数据培训

数据仓库　物流运费价..

数据仓库 olap

电脑编程入门

kerberos　linux红帽..

数据可视化

ios工程师月薪

数据分析培训班

web前端工程师

linux红帽认证

linux的学习

自学平面设计

电脑编程入门自学

运维工程师待遇

大数据培训　珠海长隆..

linux运维

阅读更多：　百度　百度　百度　百度　百度

看过本文的人还看过

美国代理服务　集成墙饰　电脑编程入门

集成灶　大数据学习　三室二厅样板

室内设计学习　联排别墅装修　数据分析培训

嵌入式学习路　html5教程　大数据培训

万科城户型　国外网站设计

authentication　hadoop数据仓库

一室一厅出租　青年公寓租房

小户型复式楼　学英语从零开始

三室二厅样板房　回龙观租房

动态口令　如何安装ipa　免费云服务器

linux培训　数据分析　太阳公元二手房

集成墙板　全自动过滤器　分布式系统

数据分析培训班　智能停车场系统

迷你主机　找过滤器　集成电视墙

linux学习　自清洗过滤器　联排别墅..

linux系统修改　linux系统

集成　集成灶　Linux教程　万科城户型

国外网站设计　authentication

hadoop数据仓库　一室一厅出租

青年公寓租房　小户型复式楼

学英语从零开始　三室二厅样板房